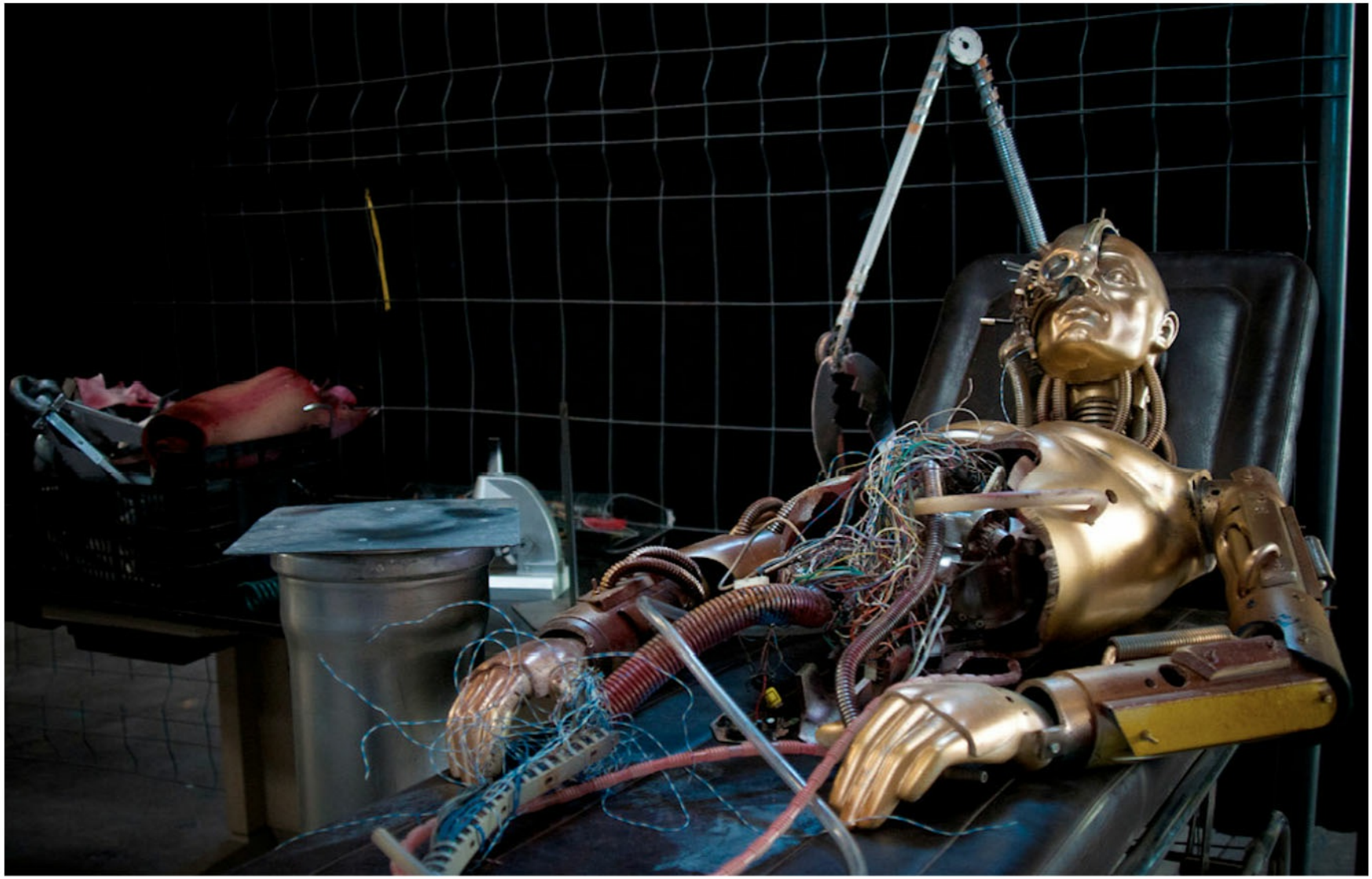
SABINE BLANC - OPHELIA NOOR
HACKERS:
BÂTISSEURS
DEPUIS
1959
OWNI
ÉDITIONS
Livre
numérique

SABINE BLANC - OPHELIA NOOR

HACKERS : BÂTISSEURS DEPUIS 1959

"Le contournement intelligent des limites imposées, qu'elles le soient par votre gouvernement, vos propres capacités ou les lois de la physique."

Jude Milhon, "St. Jude", patronne des hackers, 1939-2003



Soulever le capot, un des fondement de la culture hacker. Un des nombreux robots du Tetalab (THSF), le hackerspace de Toulouse, dans ses locaux partagés avec le collectif d'artistes Mix'art Myris.

DIS, C'EST QUOI UN HACKER ?

Les hackers n'ont pas de chance : toute communauté a ses brebis galeuses, sans pour autant que les brebis galeuses ne finissent par devenir, dans l'opinion, la communauté en elle-même. Un peu comme si médecin avait fini par signifier "charlatan". Assimilé à des actes répréhensibles, comme le médiatique piratage de carte bleue, le hacking est désormais entendu comme une pratique négative. Soit un contre-sens parfait.
Un hacker, *stricto sensu*, est une personne qui fait un usage créatif des techniques pour qu'elles répondent à son besoin, en les détournant de leur finalité initiale. Il n'y a aucune notion d'illégalité dans le terme. On peut faire le parallèle avec un couteau : sa fonction est de trancher. La viande ou la gorge de votre voisin. Mais en lui-même, il n'est ni bon, ni mauvais.
Il existe d'autres termes pour préciser avec quelles intentions un hacker déploie son habileté. Pour décrire un vilain hacker, il convient d'employer "black hat" ("chapeau noir") ou "cracker". Un gentil hacker s'appelle aussi un "white hat" ("chapeau blanc"). Et au milieu, se trouvent les "grey hats", parfois du côté obscur de la force, parfois du bon côté. Une dénomination tout droit tirée... du vocabulaire des jeux de rôles, qui comptent de solides fans dans les rangs des hackers. Attribuer ces couleurs n'est pas toujours simple : certains jugent parfois nécessaire de commettre des actes répréhensibles du point de vue de la loi au nom d'intérêts jugés éthiquement supérieurs, comme la liberté de communication. Tout en bas de l'échelle, on trouve les "script kiddies", littéralement des "gamins du script" car ils récupèrent des scripts (un petit programme) sans en créer.
Le hacking est une véritable culture et un état d'esprit, qui a ses codes, sa hiérarchie, son éthique. Dans ce sens, il peut s'appliquer à n'importe quel domaine, même si le coeur initial touche la technique, et en particulier le code informatique. Le célèbre hacker Eric S. Raymond[1], mettait les choses au clair dans son essai Comment devenir un hacker :
"L'état d'esprit d'un hacker ne se réduit pas à cette culture des hackers du logiciel. Il y a des gens qui appliquent l'attitude du hacker à d'autres domaines, comme l'électronique ou la musique. En fait, on trouve cet esprit à l'état le plus avancé dans n'importe quel domaine de la science ou des arts.
Les hackers du logiciel reconnaissent cette similitude d'esprit, et certains affirment que la nature même du hacker est indépendante du domaine particulier auquel le hacker se consacre réellement."
Le vrai hacker exalte l'ingéniosité, l'esprit de détournement, la créativité, la beauté gratuite du geste et l'élégance dans la réalisation, son code relève de l'art - "code is poetry" - car il est l'expression de la personnalité ; il défend la liberté d'information et le partage des connaissances, nécessaires pour progresser : *"the information wants to be free"*. [2]
Il dédaigne les hiérarchies conventionnelles, et leur préfère la *do-ocracy*, c'est-à-dire le respect de celui qui fait et non de celui qui se drape dans de grands discours incantatoires ; il ignore les 35 heures, car un hacker est un passionné qui ne compte pas son temps quand il s'agit d'aller au bout de son idée.[3]
À l'opposé du bûcher médiatique, le hacking est aussi perçu comme une activité sexy et tendance, qui va de pair avec le retour en grâce du geek - encore un mot vendu à toutes les sauces. Le hacking subit un phénomène de dilution de son sens. Dès qu'il y a action un peu audacieuse, inattendue, ingénieuse, on va parle de hack. *"J'ai hacké la recette de poulet thaï de Marmiton.org en mettant de la coriandre en plus" ; "j'ai hacké le salon en mettant le fauteuil à la place du canapé"*, etc. Et soyons honnête, *Owni* peut verser dans ce plaisir coupable...
Diabolisation ou exaltation témoignent du pouvoir d'attraction de ces bidouilleurs nimbés de leur aura de magicien de la technique. Dans une société où la technique innerve chaque part de notre existence, même sur le plateau du Larzac, cette culture hacker relève in fine de la politique, au sens propre du terme, *polis* en grec, la cité organisée. *"Le grand public ne voit pas en quoi le contrôle de la technologie est une question politique"*, déplorait Benjamin Mako Hill, chercheur au MIT[4] Certains hackers entrent même

dans le bal de la politique. Peu importe. Le fait est que cette communauté constitue un terreau de réflexion extraordinairement fertile depuis plusieurs décennies. Elle constitue un écosystème où se dessine des modèles alternatifs.

Ce livre n'a d'autre prétention que de vous offrir un panorama de ce que cette communauté a apporté au monde moderne, à travers ses grandes innovations et quelques figures marquantes. Nous parlerons beaucoup d'éthique car cette contribution des hackers à la cité est indissociable de cet ensemble de valeurs. Non sans nuances voire tensions d'un groupe à l'autre. Il sera ainsi beaucoup question de technique, mais en mettant toujours l'accent sur la philosophie qu'elle incarne.

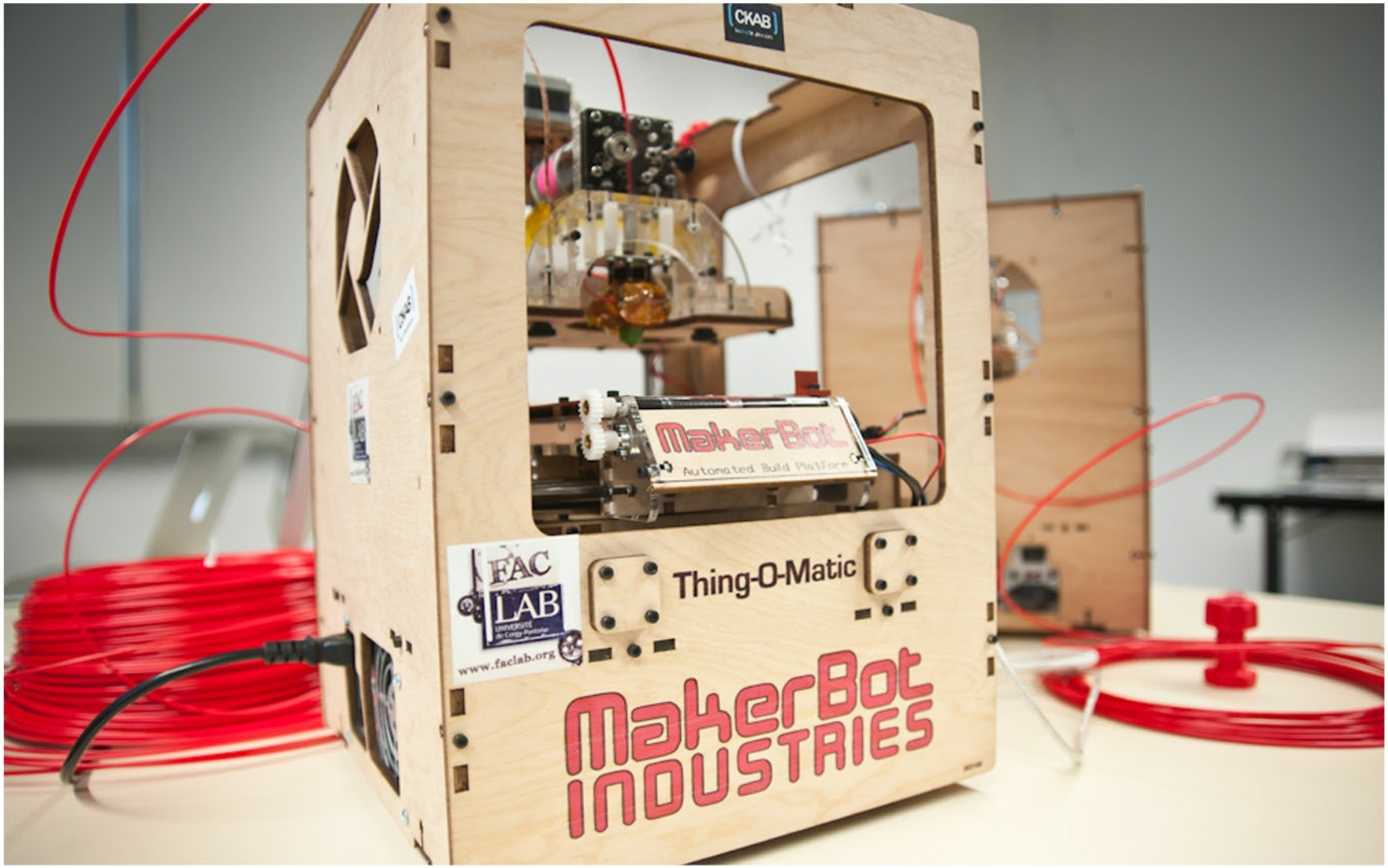
Notre petit voyage commence à la fin des années 50, dans l'Amérique blanche, à l'ombre des laboratoires, dans les lignes de code. Il se finit aux quatre coins de la planète, dans notre monde bien tangible, dans des lieux ouverts au public et même sous les lumières crues du Parlement européen. Une fin provisoire : tant qu'il y aura des esprits libres et curieux, il y aura des hackers.

Pourquoi partir de 1959 ? Puisque le hacking est un état d'esprit, nous aurions effectivement pu remonter à l'Antiquité, avec la figure de Socrate par exemple. Le philosophe Pekka Himanen, un des auteurs de *L'éthique hacker*, le considère comme son hacker préféré :

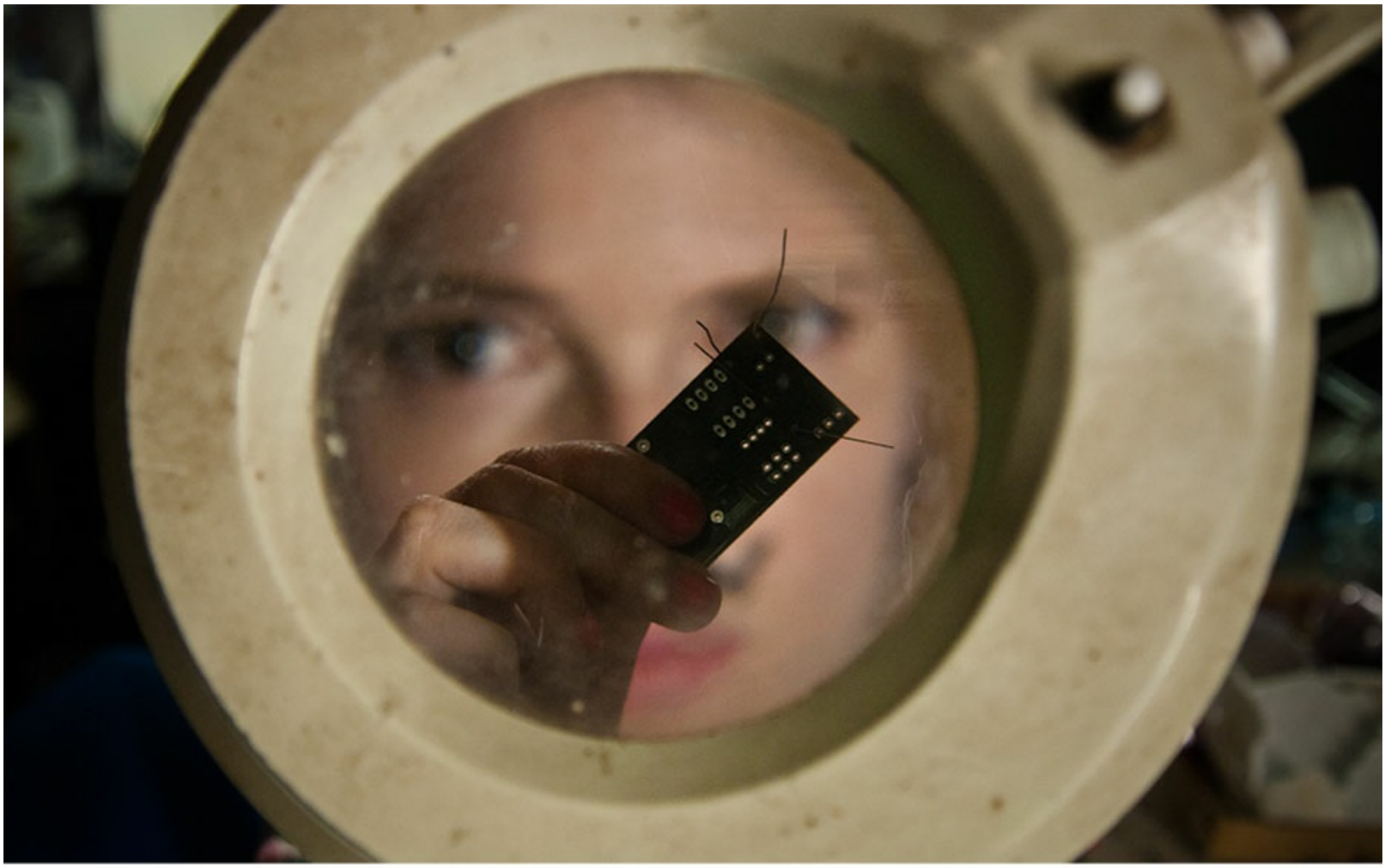
"Toute son attitude, cette relation passionnée et modeste au savoir, son ouverture d'esprit, sa quête de directions intellectuelles non prévues : l'attitude des Grecs anciens est très similaire à celle des hackers d'aujourd'hui. Platon, son disciple, a fondé la première académie du monde occidental, et c'est le modèle de la recherche scientifique aujourd'hui. C'est aussi celui des hackers passionnés d'ordinateurs..." *[5]*

Nous avons tout simplement pris pour point de départ un prétexte sémantique : le terme, qui signifie à la base "tailladder", aurait été entendu dans ce sens pour la première fois en 1959, au Massachusetts Institute of Technology (MIT) à Boston. Les membres du Tech Model Railroad Club (TMRC), des mordus de petits trains, passaient des heures à bâtir un réseau ferroviaire à la mesure de leurs envies. Le hacker taillade, met en pièces un système et en construit un nouveau. Un enfant qui ne suit pas le plan du modèle de LEGO proposé est une graine de hacker...

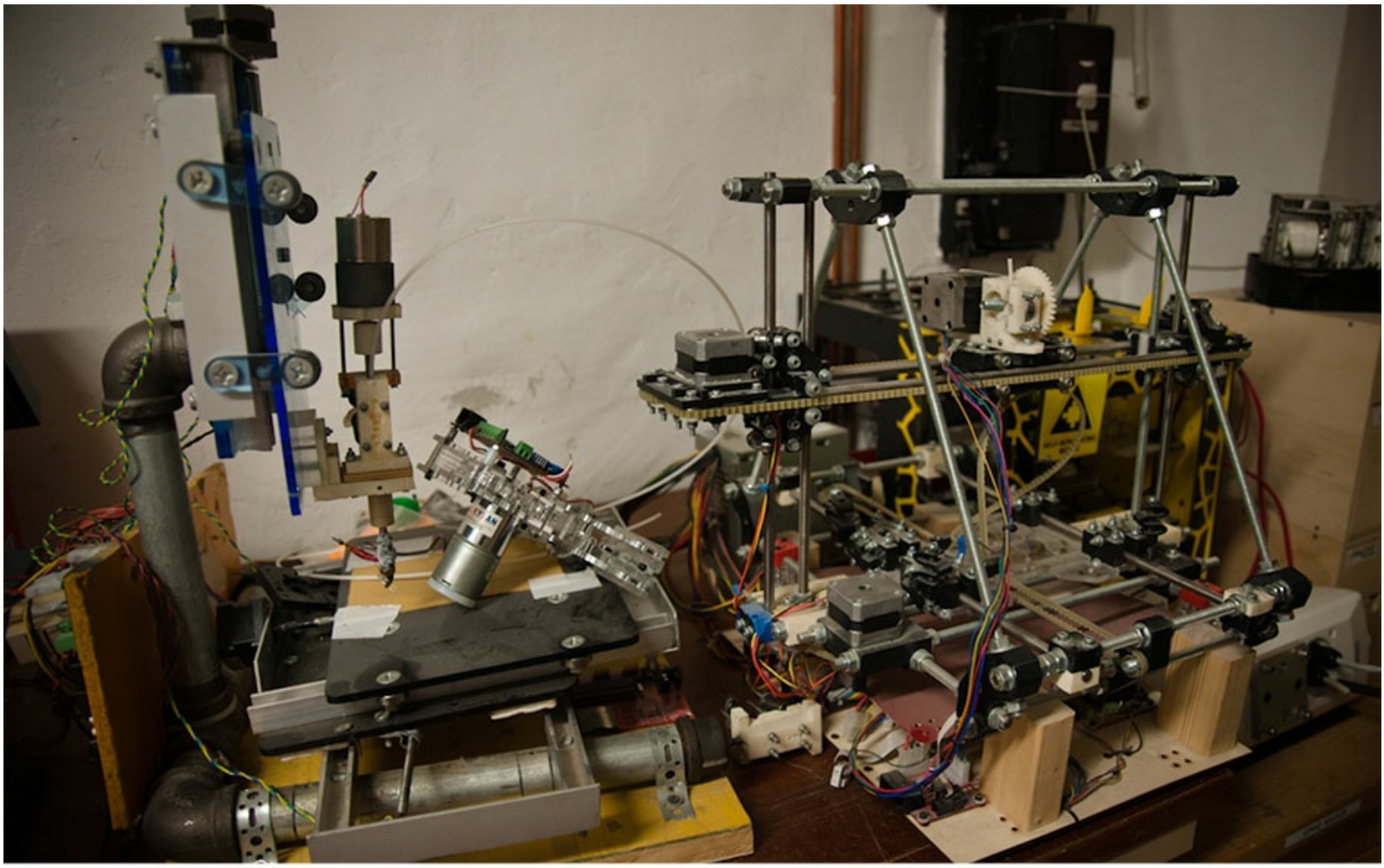
ENTREZ DANS LEUR MONDE, CE SONT DES HACKERS...



L'imprimante 3D MakerBot pur produit du hacking, dont les premiers prototypes ont été réalisés au Metalab, le hackerspace de Vienne (Autriche), par Bre Pettis, avant d'être achevée au hackerspace NYC Resistor. C'est aujourd'hui un des instruments phare des fab lab et hackerspaces.

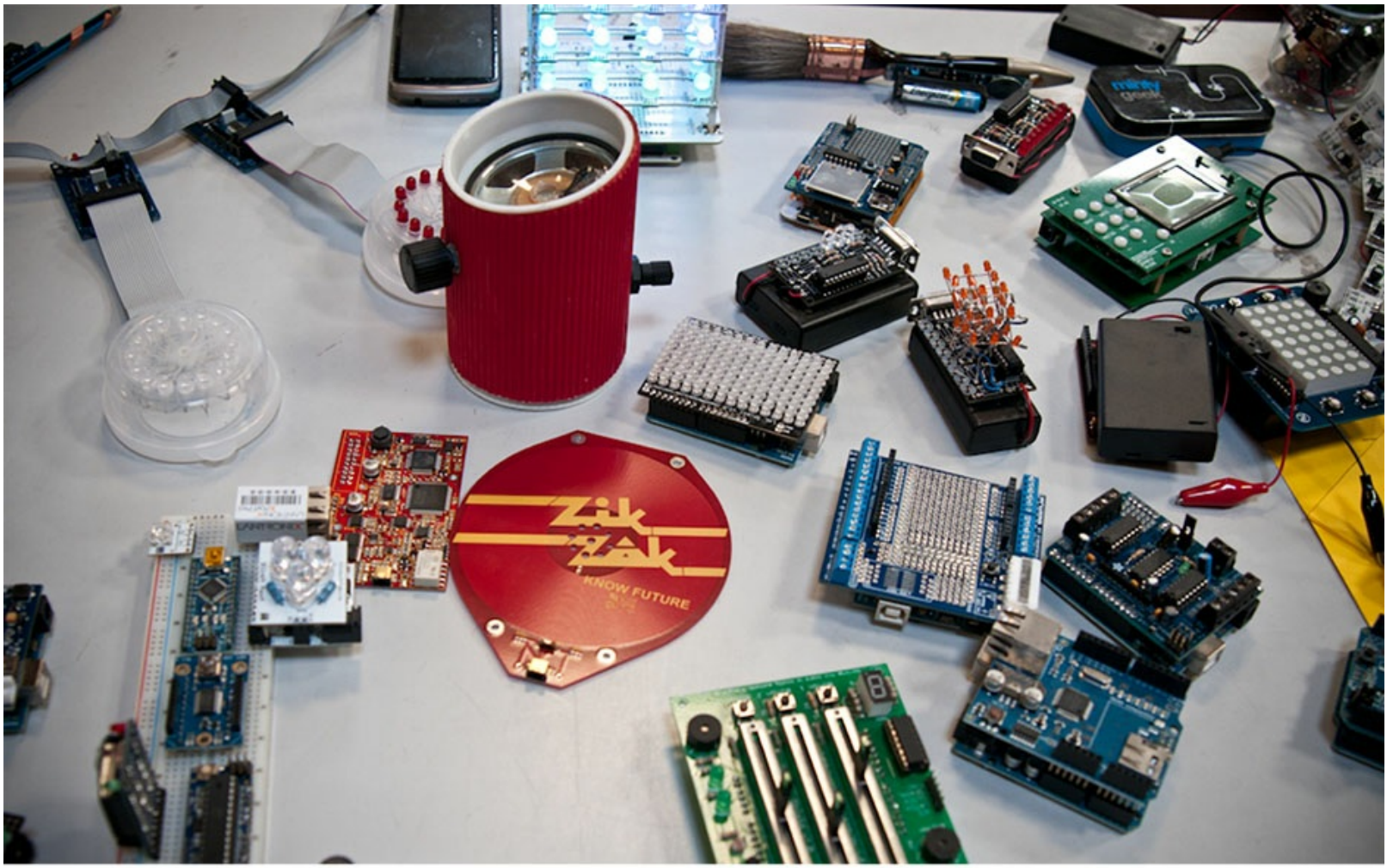


Toulouse, mai 2011. Laura, a croisé le chemin du Tetalab, le hackerspace toulousain, pendant ses études aux Beaux-Arts. Entre D.I.Y, transdisciplinarité et sens de l'indicipline, Laura a trouvé sa place.



Les premiers prototypes de l'imprimante 3D MakerBot au Metalab, le hackerspace de Vienne, Autriche.

Finowurt, près de Berlin, août 2011. Atelier soudure entre père et fils conduit par le hacker Mitch Altman au Chaos Communication Camp. Le CCC, le plus grand rassemblement de hackers au monde, a lieu tous les quatre ans.Mitch Altman a publié en Creative Commons un petit guide (.pdf) de la soudure facile (“soldering is easy”).



Circuits imprimés, au Tetalab, le hackerspace de Toulouse.

I. DES LABORATOIRES AUX GARAGES

“Il existe une communauté, une culture partagée, de programmeurs expérimentés et de spécialistes des réseaux, dont l’histoire remonte aux premiers mini-ordinateurs multi-utilisateurs, il y a quelques dizaines d’années, et aux premières expériences de l’ARPAnet. Les membres de cette culture ont créé le mot “hacker’’. Ce sont des hackers qui ont créé l’Internet. Ce sont des hackers qui ont fait du système d’exploitation Unix ce qu’il est de nos jours. Ce sont des hackers qui font tourner les newsgroups, Usenet et le World Wide Web.”

Cette histoire de l’apport des hackers à l’informatique moderne qu’Eric S. Raymond [6] nous retrace d’un paragraphe définitif commence derrière les murs des universités à la fin des années 50, quand les ordinateurs étaient accessibles à une poignée de privilégiés, étudiants, chercheurs, ingénieurs.

Une quinzaine d’années d’innovations plus tard, cette histoire va rejoindre les foyers et prendre, déjà, une tournure politique. Souvent oubliées, ces premières années sont pourtant fondatrices car cette incroyable créativité est inséparable des valeurs que cette communauté cristallise alors.

LES DÉFRICHEURS DU M.I.T [7]

TOUS LES PETITS TRAINS MÈNENT AUX ORDINATEURS

Peter Samson, Alan Kotok, Bob Saunders, Jack Dennis : ces noms sont inconnus du grand public, qui n’a retenu de l’histoire de l’informatique que les trajectoires dorées de Bill Gates ou Steve Jobs. Pourtant, sans ces jeunes bidouilleurs surdoués, vous ne seriez tout simplement pas en train de lire cet ebook. Parce que, habitué au -faux ? - confort de nos machines fermées, où le code ne se voit plus, comme le capot couvre le moteur, nous avons oublié que fut un temps où ouvrir le capot était indispensable. Et l’histoire des hackers nous montrera qu’il est dangereux de penser qu’on peut définitivement faire l’économie de cette curiosité.

Revenons à nos premières cartes perforées. Carte perforée et non ligne de code car l’histoire de l’informatique grand public trouve ses racines voilà 50 ans, au Massachusetts Institute of Technology (MIT). Aujourd’hui l’ordinateur est un objet bien banal dont on se débarrasse dès qu’il présente des signes d’obsolescence. En 1959, même dans un lieu aussi pointu que le MIT, pour un esprit aussi curieux que Peter Samson, c’est un objet de fascination sans fin, un monument devrait-on dire. Les systèmes d’alors, baptisés *mainframe*, sont centralisés, occupent une pièce entière, ne possèdent pas d’écran, les programmes s’écrivent sous forme de carte perforée et il faut imprimer le résultat des calculs. Mais les champs qu’ils ouvrent sont infinis, et peu importe qu’ils soient sexy comme un bahut.

Peter Samson, 18 ans, est un des passionnés de notre club de modélisme ferroviaire, le TRMC, *“un hacker du MIT, un des premiers, qui aimait les systèmes, les trains, TX-0, la musique, la procédure parlementaire, les blagues de potaches et le hacking”*, décrit Steven Levy dans son ouvrage de référence *Hackers, heroes of the computer revolution. “Peter Samson et ses amis avaient grandi avec une relation particulière au monde, où les choses avaient du sens uniquement si vous trouviez comment elles fonctionnaient. Et comment y parvenir si ce n’est en mettant la main à la pâte.”*

Le TRMC est alors divisé en deux grands groupes : les mordus de modélisme et ceux qui s’occupent des circuits, le “Signals and Power Subcommittee” (le sous-comité signaux et puissance). C’est au sein du S&P que la culture hacker va naître, de leur envie immodérée d’améliorer leurs circuits qui les amène à s’intéresser aux ordinateurs, une sérendipité[8], appliquée à la technique, sans se soucier des cloisons, réelles ou métaphoriques.

Le bâtiment 26 est particulièrement attrayant : il abrite la salle Electronic Accouting Machinery (EAM) avec sa machine à carte perforée, sa connexion avec l'ordinateur IBM 704. Mais la bête est frustrante : il faut passer par des opérateurs intermédiaires pour perforer les cartes mais aussi les exécuter, une procédure lourde appelée "traitement par lots". En revanche, l'IBM 407 leur permet de bidouiller en totale autonomie : *"Elle pouvait faire ce que vous vouliez qu'elle fasse. [...] Ce fut parmi les premières escapades de hacker informatique du Tech Model Railroad Club."*
Juste en-dessous, on trouve le Radio Laboratory of Electronics (RLE) où un des premiers ordinateur à transistors, le TX-0, a échoué après avoir fait son temps. Quand Jack Dennis, un ancien membre du TMRC qui a travaillé dessus, leur propose d'y accéder, c'est l'extase : cette machine fonctionne sans carte, grâce au Flexowriter, un ancêtre du clavier qui permet de taper directement son code.
Ce qui facilite infiniment la vie : les hackers interagissent directement avec la machine, les erreurs sont plus vite repérées et débugguées, c'est-à-dire corrigées.
Nos proto-hackers se lancent dans la programmation grâce au premier cours sur le sujet à destination des nouveaux entrants proposé par le MIT au printemps 1959. Ils découvrent le LISP, un nouveau langage de programmation créé par le professeur John Mac Carthy, l'inventeur de l'intelligence artificielle. Lui fait des plans sur la comète, eux préfèrent transpirer sur le code pour l'améliorer encore. En revanche, quand Mac Carthy se prend de passion pour l'élaboration d'un jeu d'échec, ça fait ping, et Alan Kotok en fera même sa thèse. Plus tard, les hackers du TRMC formeront le coeur des troupes du laboratoire d'intelligence artificielle (IA) à Tech Square, pionnier dans le domaine.
Les prémisses de la révolution numérique sont là, parfois sans autorisation. L'accès aux machines est en effet encadré et passer entre les mailles du filet fait aussi partie du jeu. Ce sera une des constantes du milieu hacker que de flirter avec les limites officielles. Un esprit curieux ne saurait s'arrêter à la ligne tracée en Haut. Quant à un autre tropisme de l'imaginaire lié aux hackers, les longues nuits passées devant la machine, il a une cause pragmatique : la nuit, les machines sont libres.
Les bonnes relations au sein du TRMC en font les frais car les hackers ont déplacé le centre d'intérêt des petits trains à la programmation : tel "un cheval de Troie", la section S&P a aussi hacké les réunions, *"exploit[ant] tous les méandres de la procédure parlementaire (sic, ndlr) pour aboutir à une réunion aussi alambiquée que les programmes qu'ils hackaient sur le TX-0."* Un quart de siècle plus tard, des collectifs de hackers feront du hack législatif un sport de combat.[9]
Le meilleur moyen de se livrer à sa passion, c'est d'en faire son métier, et tout au long des années 60 et 70's, les hackers contribuent au développement de l'informatique, qui dans un labo d'université, qui dans une entreprise, beaucoup aussi sur leur temps libre, la nuit. Au gré de leurs carrières, ils disséminent cette culture originelle née dans le berceau du MIT.
Progressivement, les chevaux des hackers se dégrossissent, grâce aux progrès de l'électronique. En parallèle des *mainframes*, les mini-ordinateurs font leur apparition, l'étape d'avant le micro-ordinateur que nous connaissons. Les machines de la société DEC ont largement leurs faveurs, face à celles d'IBM qui symbolisent une vision bureaucratique, contrainte, de la programmation.
Ils jettent leur dévolu sur la série PDP, dont le premier rejeton, PDP-1, l'héritier de TX-0, dispose d'un écran qui facilite bien la vie. Editeur de texte, traitement de texte, programmes de debugging pour repérer et corriger les erreurs, programme de musique, la liste des innovations est longue, dans une ambiance de (mâle) émulsion amicale où chacun rivalise de prouesses, dans un rapport presque sensuel à la machine.
Et comme les hackers aiment s'amuser, ils développent en 1962 un des premiers jeux vidéo, *Spacewar!*[10] Si l'histoire a retenu le nom de Steven Russell, son développement complet est le fruit d'un travail collectif. *Spacewar!* illustre à merveille la notion de hack puisqu'il est né de l'exploitation d'une erreur. Minsky, un des hackers de la petite bande, travaille sur un programme d'affichage qui transforme des lignes droites en des courbes. Une faute de frappe, et voilà qu'un cercle se trace. Amélioré, cet algorithme génère des formes interactives. Un fascinant spectacle à l'époque qui tape dans

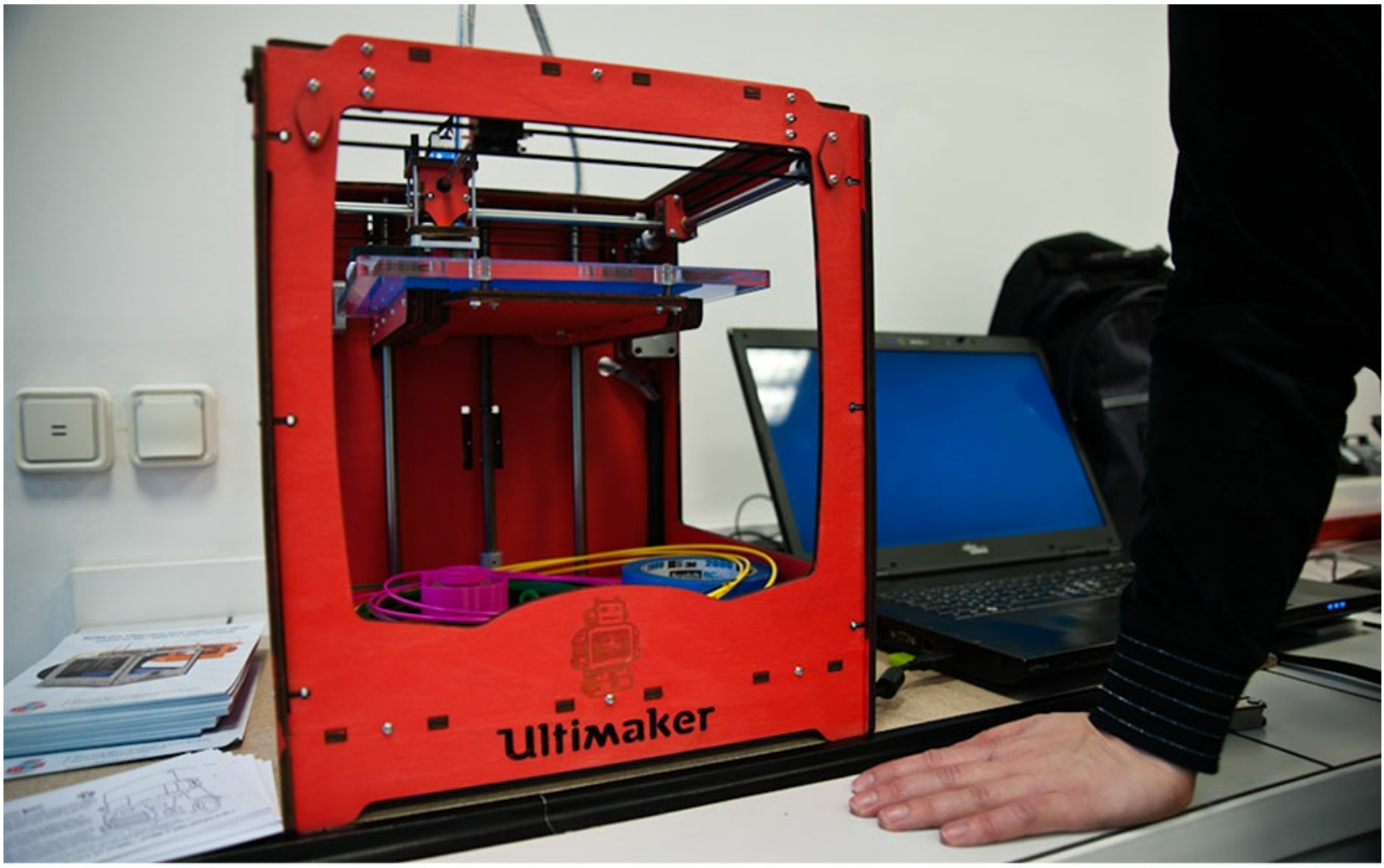
l’esprit passionné par la science-fiction, et en particulier le space opera, de Steve Russell. Des centaines d’heures de hack plus tard, il en sort *Spacewar!*
Bien avant *Counter Strike*, ce frustre jeu donne lieu à d’interminables parties, litres de Coca à l’appui, ce qui les conduit tout naturellement à élaborer le premier joystick pour soulager les coudes endoloris, à partir de... pièces du TRMC. Ils ne sont pas les seuls à découvrir les joies du gaming : d’université en université, le jeu circule. Mieux encore, dès 1969, Rick Blomme code une version qui permet de jouer à deux via le réseau universitaire PLATO, soit le premier jeu en ligne de l’histoire.
Quant au grand public, il ressort médusé de leur démonstration sur grand écran lors des journées portes ouvertes en 1962 : *“La vue de cela, un jeu de science-fiction écrit par des étudiants et contrôlé par un ordinateur était si proche du rêve que personne n’osait prédire qu’il engendrerait un genre à part entière de divertissement.”*
Une décennie plus tard, en 1971, un ingénieur pétri d’ambitions du nom de Nolan Bushnell marque le début de l’industrie du jeu vidéo avec son adaptation de Spacewar! qu’il commercialise sous le nom de Computer Space en 1971. Ce sera un échec mais sur les décombres de cette première mésaventure, il créera en 1972 Atari et sa borne Pong qui fera un carton. Le lucrative business du jeu vidéo peut vraiment commencer.
Moins ludique mais tout aussi important, le concept de *time-sharing* (“temps partagé”) fait l’objet de grandes attentions. Le but est d’optimiser l’utilisation de la ressource machine en permettant à plusieurs personnes de travailler en même temps dessus. Le projet MAC lui est dédié au laboratoire d’AI avec le soutien de l’Advanced Research Projects Agency (Arpa), l’agence de recherche du Pentagone, qui a bien compris l’intérêt des ordinateurs en terme d’applications militaires. Une première version “officielle” est développée, *Compatible time-sharing system* (CTSS), sur une machine de la marque IBM tant haïe.
En réaction, les hackers proposent leur version, qu’ils nomment *Incompatible time-sharing* (ITS) par ironie, car elle incarne la quintessence de l’éthique hacker : pas de mot de passe, système de fichier partagé préfigurant nos wikis d’aujourd’hui. Elle offre la possibilité au même utilisateur de faire tourner plusieurs programmes en même temps et un système d’editing plein écran.
Si ITS n’est pas retenu comme standard pour la prochaine machine de DEC, il servira à développer des logiciels importants jusque dans les années 90, démontrant que l’éthique hacker a de beaux jours devant elle.

DÉCONNECTÉS

Durant ces années, les innovations du MIT sont indissociables d’une éthique implicite qui guide leurs explorations, un ensemble de valeurs qui façonne leur appréhension du monde et en particulier de la technique.
Ainsi, lorsque Steven Nelson, un petit nouveau dans la bande, leur fait découvrir les joies de ce qu’on appellera plus tard le phreaking, c’est-à-dire le hack des réseaux de télécoms, il évacue toute notion de profit autre qu’intellectuel :
*“Mais même quand Nelson partait dans ses voyages électroniques, il adhérait à la morale hacker officieuse. Tu pouvais appeler partout, essayer tout, expérimenter sans cesse, mais tu ne devais pas le faire pour le gain financier. Nelson désapprouvait ces étudiants du MIT qui construisaient du matériel à “blue boxes” pour faire des appels illégaux dans le but d’arnaquer les opérateurs de téléphonie[11]. Nelson et les hackers pensaient qu’ils *aidaient* les opérateurs de téléphonie. Ils voulaient mettre la main sur leurs numéros d’appel prioritaires dans différents endroits du pays et les tester. Si cela ne fonctionnait pas, ils le rapportaient au service de réparation approprié.” [12]*
Liberté est le maître-mot : par défaut les programmes sont ouverts, circulent de main en main car ils ne constituent pas une économie. La copie n’est pas un crime, c’est un droit et un devoir, un cercle vertueux grâce auquel progresser. Et quand bien même les programmes seraient déjà la cash machine qu’ils sont

devenus, l'idée n'effleure même pas les hackers :
"Samson présenta fièrement le compilateur de musique à DEC pour le distribuer à quiconque le voulait. Il était fier à l'idée que d'autres personnes utiliseraient son programme. L'équipe qui travaillait sur le nouvel assembleur pensait de même. Par exemple, ils étaient contents d'avoir la bande perforée du programme dans un tiroir si bien que toute personne utilisant la machine pourrait y accéder, essayer de l'améliorer, en tirer quelques instructions ou y ajouter des fonctionnalités. Ils se sentirent honorés quand DEC leur demanda le programme pour pouvoir le donner aux autres possesseurs de PDP-1. La question des royalties ne se posa jamais. Pour Samson et les autres, utiliser l'ordinateur était une telle joie qu'ils auraient payé pour cela. Le fait d'être payé la royale somme de 1.60 dollars par heure pour travailler dessus constituait un bonus."
Et quand Steve Russell y songe un instant, le jeu a déjà été repassé à DEC, à la grande joie des ingénieurs de PDP-1 qui testent la machine dessus.
Ce même goût pour la liberté les pousse à se prendre de passion pour le crochetage de serrure. Ils peuvent ainsi accéder à toutes les pièces et à tout le matériel qu'ils souhaitent et commencer à hacker le hardware, le matériel :
"Pour un hacker, une porte fermée est une insulte, et une porte verrouillée un outrage. [...] Quand un hacker avait besoin de quelque chose pour l'aider à créer, explorer ou réparer, il ne s'embêtait pas avec des concepts aussi ridicules que la propriété intellectuelle. [...] Le passe-partout était plus qu'un outil pour accéder ses fins : c'était un symbole de l'amour des hackers pour le libre accès. [...] Les verrous symbolisaient le pouvoir de la bureaucratie, un pouvoir qui serait finalement utilisé pour empêcher la mise en oeuvre de l'Ethique Hacker. Les bureaucraties étaient toujours menacées par les gens qui voulaient savoir comment les choses marchaient. Les bureaucrates savaient que leur survie dépendait du maintien dans l'ignorance des gens, en utilisant des moyens artificiels comme les verrous pour les garder sous contrôle." [13]
Mais ils ne réfléchissent pas à l'impact sociétal et politique des machines. Ils vivent, déconnectés, dans leur bulle, tout à leur art ; leur mode de vie exaltant la décentralisation et la liberté a un parfum inconscient d'anarchisme à la sauce technophile : les hackers croient profondément que les machines sont un vecteur de progrès. S'ils sont plutôt opposés à la guerre, leurs actions en tant qu'hacktivistes font pâle figure en comparaison de ce que feront leurs héritiers 40 ans plus tard lors des révolutions arabes.[14]
À grands coups de manifestations pacifistes devant Tech Square, la guerre du Vietnam leur rappelle brutalement à la fin des années 60 leurs profondes contradictions : le laboratoire d'AI est financé par les militaires. Et sur ce point, nos hackers éthiques se montrent plutôt louvoyants dans leurs explications.
En revanche, sur la côte opposée, pacifisme, libertarisme, anarchisme et esprit d'entreprise forment un cocktail politico-économique détonnant qui fera le succès de la Silicon Valley : le temps de l'ordinateur pour tous approche.

La récupération, tout un art : des tours centrales et des moniteurs en pagaille au Loop, un des hackerspaces de Paris, dans un immeuble squatté de la rue Chapon (Paris 3ème) pendant l'été 2011.



L'Ultimaker, une autre imprimante 3D développée au Protospace, le fab lab d'Utrecht aux Pays-Bas.

FAITES DES ORDINATEURS, PAS LA GUERRE

FLOWER POWER HACKER[15]

À des milliers de kilomètres du MIT, en Californie, une nouvelle génération de hackers bourgeonne dans le milieu de la contre-culture pacifiste. Alors que les hackers du MIT ont en horreur la cigarette, les contours idéologiques de la cyberculture des années 90 s'esquissent dans des volutes de fumées psychédéliques. Le futur pape de la cyberculture, Timothy Leary, vante la libération par les drogues, prophète sous hallucinogènes. 20 ans plus tard, il proclamera que "*le PC est le LSD des années 90*". Préfigurant Wikipedia, le *World Earth Catalog*, édité par Stewart Brand, est une caverne d'Ali-Baba dont le contenu ne dément pas la promesse de son titre : on y parle de tout.

Plus personne ou presque ne se souvient de cette publication maintenant, mais elle aurait "*créé les conditions culturelles grâce auxquelles les micro-ordinateurs et les réseaux informatiques auraient été perçus comme les instruments de cette 'libération' "* pour Fred Turner, l'auteur de *From counterculture to cyberculture.[16]*

Loin de voir dans les ordinateurs des machines de mort, comme certains pacifistes, ou de rester enfermés dans la tour d'ivoire d'un laboratoire, les hackers issus de cette communauté y voient au contraire un outil d'empowerment démocratique sans précédent. Computer Lib, un livre-manifeste écrit par Ted Nelson, affiche en couverture un poing levé qui annonce des lendemains qui chantent sur un rythme binaire. Quelques années auparavant, le jeune homme a mis en route un projet aussi titanesque que pionnier, Xanadu. Il imagine une bibliothèque géante dématéralisée, fonctionnant sur un principe récent qu'il baptise hypertexte, et qui trouvera un quart de siècle plus tard son aboutissement avec le world wide web.[17]

Autour de ce motto se croise et échange une poignée de communautés qui va prendre en main cette

évangélisation des masses qu'ils appellent de leurs voeux. Il y a par exemple Ressource One Collective qui pense que *"les outils technologiques peuvent être les outils d'un changement social s'ils sont contrôlés par les gens.*" Ou bien encore celle qui gravite autour de People's Computer Company, une newsletter lancée par Bob Albrecht et George Firedrake en 1972. Le texte de sa première couverture est aussi éloquent :

"Les ordinateurs sont principalement utilisés contre les gens et non dans l'intérêt des gens
Utilisés pour contrôler les gens et non pour les libérer
Il est temps de changer tout cela nous avons besoin d'une Compagnie informatique des gens"
("People's Computer Company")

En 1972, la petite bande du Community Memory Project marque un coup avec une innovation qui démontre, concrètement, que l'ordinateur n'est pas que déshumanisant mais est aussi un vecteur de lien social. Efrem Lipkin, Mark Szpakowski et Lee Felsenstein lancent cette année-là le premier Bulletin Board Service (BBS) l'ancêtre des mailing lists, à partir d'un ordinateur récupéré chez Ressource One. N'importe qui peut laisser un message taggé par des mots-clés et trouver ainsi des gens partageant le même centre d'intérêt. Avec ses hashtags, Twitter a somme toute réinventé le fil à couper le beurre... La connexion au système se fait *in real life*, dans l'espace public d'un magasin de disques de Berkeley.

DES JEUNES GENS DANS UN GARAGE

Pour que le potentiel politique de l'informatique éclose, il reste encore à créer le matériel de cette révolution à venir. À cette époque, les ordinateurs sont toujours au stade des machines envahissantes, coûteuses et complexes, inaccessibles pour un particulier, une sorte de bureaucratie technique incarnée par IBM. Simultanément, plusieurs personnes travaillent sur un projet similaire : un ordinateur en kit, qui permettra au plus grand nombre de mettre en oeuvre l'éthique hacker.

Les progrès de l'électronique et surtout sa démocratisation, couplés à ceux de la programmation, vont leur permettre de réaliser leur rêve. En 1972, Intel lance le premier micro-processeur, la puce 8008, puis une nouvelle version plus performante, la 8080. Un nouveau langage fait aussi son apparition, BASIC, dont la People's Computer Company est un fervent adepte. Comme son nom le suggère, il est conçu pour apprendre à coder. Peut-être certains d'entre vous se souviennent avoir transpiré à l'école dans les années 80 dans le cadre du projet "informatique pour tous", et bien, c'était du BASIC.

Lee Felsenstein, un passionné d'électronique qui se définit comme *"un homme de la Renaissance, un ingénieur et un révolutionnaire"*, démarre son projet. Il crée à cette fin sa compagnie, LGC Engineering, bien loin de l'esprit du grand capital : son nom est un hommage à un poème, *Loving Grace Cybernetics*, qui imagine un futur où, libéré du travail grâce à la machine, l'homme peut de nouveau vivre en fusion avec la nature.

Non loin de la Californie, au Nouveau Mexique, Ed Roberts hacke dur aussi pour mettre au point sa machine. Il bosse d'autant que sa petite compagnie, MITS, perd de l'argent. Quand il met enfin en vente sa machine au prix canon de 397 dollars, c'est la fin des vaches maigres : l'Altair 8800, baptisé ainsi en hommage à *Star Trek*, connait un succès foudroyant grâce à la publicité gratuite que lui fait le magazine *Popular electronics* en le présentant dans son numéro de janvier 1975.

N'imaginez pas non plus des hordes d'ordinateurs débarquer du jour au lendemain dans les foyers. Construire un kit n'est pas une sinécure, même pour des amateurs enthousiastes. Un bon vieux club devrait débugguer quelques problèmes : ce sera le Homebrew Computer Club, créé par Fred Moore et Gordon French, deux habitués du PCC.

Le Homebrew Computer Club rassemble *"la plus belle collection d'ingénieurs et de techniciens que vous pouviez réunir sous un toit."* Et le toit en question, au début, c'est vraiment celui d'un garage, chez French Gordon. Si le HCC est passé à la postérité pour avoir donné naissance à des géants de l'informatique, pour l'heure, l'esprit hacker imprègne les réunions. Steve Wozniak, le futur cofondateur

d'Apple qui n'est alors qu'un salarié d'Hewlett Packard se souvient de cette ambiance si conviviale : *"Le thème du club était 'donnez pour aider les autres'. Chaque session commençait par une sorte d'inventaire lorsque les personnes se levaient, une à une, et parlaient d'une rumeur, ou d'un sujet auquel elles s'intéressaient, avant d'en discuter avec les autres. Quelqu'un affirmait 'j'ai un nouvel élément', une personne déclarait avoir de nouvelles données ou demandait aux autres membres si quelqu'un détenait un télétype. Pendant la 'période d'accès aléatoire' qui a suivi, on se baladait dehors et on tombait sur des personnes qui échangeaient des appareils ou des informations et qui s'aidaient mutuellement. De temps en temps, un type se pointait et demandait 'y'a-t-il quelqu'un d'Intel ici ? Non ? Bien, j'ai quelques puces informatiques d'Intel que nous pourrions nous répartir.' Ça, c'était avant la naissance des grosses entreprises informatiques et qu'il soit question de gros sous."*

Trituré dans tous les sens par les membres du club, le mythique Altair 8800 sert de point de départ pour innover, dans un esprit de saine émulation. L'idée qu'il est possible de monter une entreprise dans l'esprit de l'éthique hacker est vivace. Quand Apple vend son premier ordinateur en 1976 sur la base d'Altair, la société est vraiment aussi cool que son logo en forme de pomme multicolore le suggère : *"Lorsque j'ai conçu les Apple I et II, c'était un passe-temps, je faisais ça pour le fun, pas pour les commercialiser. Ils étaient destinés à être ramenés au club, à être posés sur la table en période d'accès aléatoire et servaient de démonstration : 'Regardez ça, ça fonctionne avec très peu de puces électroniques'. Ils avaient un écran vidéo. Vous pouviez écrire des trucs dessus. Les claviers de PC et les écrans vidéo n'étaient alors pas très aboutis. J'étalais un peu ma science auprès des autres membres du club. Les schémas de l'Apple I circulaient librement, et je me rendais même chez les gens pour les aider à construire le leur."* [18]

La première Computer Faire (foire aux ordinateurs) en 1977 incarne cette idée que l'idéal hacker porté par le business est la meilleure façon de changer positivement le monde. Mais déjà le vent tourne, comme le prédit cette conférence hallucinée de Ted Nelson intitulée "Ces deux inoubliables prochaines années" : *"Pour le moment cependant, les petits ordinateurs fonctionnent d'une manière assez magique. Ils provoqueront des changements dans la société aussi radicaux que ceux provoqués par le téléphone ou l'automobile. Les petits ordinateurs sont là, vous pouvez les acheter avec votre carte de crédit et parmi les accessoires disponibles vous trouverez les disques de stockage, des écrans graphiques, des jeux interactifs, des tortues programmables qui dessinent sur du papier de boucherie et Dieu sait quoi d'autre encore. Tous les ingrédients pour créer de l'engouement sont ici réunis. Les ordinateurs sont en passe de devenir cultes et le marché des consommateurs sera bientôt mature. Engouement ! Culte ! Marché ! Tout le monde va se précipiter. La machine américaine de fabrication de publicités va s'emballer. La société américaine va sortir de sa bulle. Et les deux prochaines années vont être inoubliables."* [19]

Déjà, deux jeunes gens ont bien signifié qu'ils voyaient surtout dans le marché des ordinateurs personnels la future vache à lait. Bill Gates et Paul Allen, nos deux jeunes ambitieux, ont développé un compilateur BASIC pour l'Altair, ce qui rend la machine plus accessible, et s'associent avec MITS : pour chaque logiciel vendu, ils touchent une commission. Ce sont les débuts lucratifs de Microsoft, en 1975. En janvier, Bill Gates écrit une *"Lettre ouverte aux amateurs" [20]*, envoyée aux membres du Homebrew Computer Club, où il assimile les hackers à des pirates : il n'a pas apprécié que son logiciel soit copié. Dix ans plus tard, l'éthique hacker aura sa revanche avec la création de GNU[21].

LE PHREAK, C'EST CHIC

Les joujoux en plastique des boîtes de céréales finissent généralement de deux façons : dans les mains d'un enfant ou à la poubelle. Quand l'un d'entre eux est arrivé par un beau jour d'octobre 69 dans les mains d'un hacker californien qui traîne ses longs cheveux à la PCC, il s'est produit une étincelle qui a

donné naissance à un objet culte de la culture hacker, qui est venu bousculer le business des opérateurs de téléphonie.
Le jouet est question est un anodin sifflet bleu qui présente la particularité d'émettre une tonalité de 2 600 herz quand on bouche un de ses trous, soit la tonalité qui permettait alors d'accéder au réseau téléphonique longue distance de l'opérateur Bell. En clair, John Draper, notre Californien qui a fait la découverte, a trouvé le moyen de passer des appels gratuitement. La première personne avec qui il entre ainsi en contact est un gamin aveugle, Joe Engrassia, qui entrera dans la légende sous le pseudonyme de "the whistler", "le siffleur", en raison de ses dons auditifs. Dans le jargon, ce piratage des lignes se nomme phreaking, contraction de "phone" et de "freak", monstre. "Freak" peut aussi s'entendre dans le sens de "mordu", "fan", et cette acceptation est aussi pleine de sens. Car John Draper, qui prend vite le pseudo de Captain Crunch, fait cela pour le plaisir de soulever le capot, en bon hacker :
"Quand j'ai commencé, j'étais essentiellement motivé par la curiosité de savoir comment la compagnie téléphonique fonctionnait. Je n'avais pas vraiment envie de les arnaquer, de téléphoner sans payer et d'échapper à des poursuites. J'étais surtout intéressé par les codes que vous pouviez composer et ce que vous pouviez faire avec une blue box, plus que de vraiment transgresser la loi et passer des appels gratuitement. Je connaissais tout un tas de façons de téléphoner sans payer, plutôt que d'utiliser la blue box." *[22]*
Il perfectionnera sa trouvaille en créant des blue boxes, qui démocratisent le phreaking dans les années 70's. Dès 1971, le magazine américain *Esquire* contribue à faire connaître la pratique avec un article intitulé "Secrets of the Little Blue Box". La justice apporte son concours involontaire au mouvement. En effet, Captain Crunch est arrêté en 1972 et envoyé en prison quatre ans plus tard, *"la plus grosse, la plus stupide des erreurs qu'ils aient faites"*. Cette arrestation préfigure le durcissement pénal des années 80. Si les hackers les plus doués sont aujourd'hui dragués par certaines entreprises, à l'époque, il n'en était rien :
"Après être allé en prison, je me suis démené pour dire à tout le monde comment procéder. Cela a entrainé beaucoup de vols aux compagnies de téléphone et cela leur a vraiment coûté beaucoup d'argent. Au fond, ils ont créé des centaines de Captain Crunch. Des milliers. Ils m'ont mis en contact avec des gens dont vous n'auriez jamais voulu qu'ils accèdent à cette technique : des prisonniers. Les prisonniers adorent ce genre de choses, ils les dévorent. Du coup, j'étais très populaire, je donnais des cours tous les jours. S'ils m'avaient laissé tranquille et m'avaient embauché, ils n'auraient jamais eu de problème, j'aurais collaboré avec eux, j'aurais gardé mes connaissances secrètes. Je me suis assuré que le mot circulerait en envoyant de prison un script à mon avocat qui l'a passé à des magazines underground. Des fanzines comme Tap *et* 2600 *recevaient constamment des informations envoyés par des gens comme moi."* *[23]*
Ironie de l'histoire, la légende dit que c'est grâce à l'argent du phreaking qu'est fondée une entreprise connue - et détestée d'une partie des hackers - pour ses produits fermés comme une huître : Apple. Steve Wozniak avait en effet lui aussi conçu une box qu'il vendait à ses camarades étudiants de Berkeley. Les bénéfices servent à acheter les composants du premier ordinateur de la marque. Captain Crunch raconte que c'est lui-même qui a expliqué à Wozniak comment marchait une blue box. Le jeune étudiant avait eu vent de cette invention via le fameux article d'Esquire et avait contacté Captain Crunch. La suite, nous la connaissons...

UNIX, LE PAPA DES OS

Dans l'ombre des laboratoires, loin des poussées révolutionnaires, les hackers n'ont pas tapé leur dernière ligne de code et apportent une nouvelle brique décisive à l'histoire de l'informatique. À la fin des années 60, les laboratoires Bell, associés au MIT et General Electrics travaillent sur un projet innovant et ambitieux baptisé Multics, un OS en temps partagé pour *mainframe*. Innovant et surtout trop

compliqué, il est mis de côté. En 1969, Ken Thompson, un des chercheurs des laboratoires Bell qui a travaillé sur Multics, décide de le retravailler dans son coin, malgré l'absence de soutien financier. Ken Thompson n'a pas envie de faire *tabula rasa* de ce projet qui a nourri sa réflexion et il est d'autant plus motivé qu'il veut pouvoir continuer à faire tourner le jeu qu'il a développé pour *Multics Space travel*.
Les recherches aboutissent en 1971 à un nouveau système d'exploitation multitâche et multiutilisateur : UNIX. La grande innovation arrive avec la quatrième version, en 1973 : recodé dans un nouveau langage de programmation, le C, UNIX est désormais portable d'une machine à l'autre.
Ce nouveau langage développé par Dennis Richie et Brian Kernighan est à la fois assez simple, généraliste et rapide pour écrire un système d'exploitation qui tourne sur n'importe quelle machine pourvue d'un compilateur C. Encore utilisé aujourd'hui, le C a donné naissance à de nombreuses variantes. Quand Dennis Richie mourra à l'automne 2011, le monde des hackers et de l'informatique moderne en général perdra une de ses figures tutélaires[24].
Comme ITS, le système en temps partagé des hackers du MIT, Unix incarne aussi une philosophie, résumée par Dennis Richie :
"Nous ne voulions pas seulement préserver un bon environnement de programmation, mais un système autour duquel une communauté pourrait se constituer. Nous savions d'expérience que l'essence de l'informatique communautaire, telle que fournie par l'accès à distance à des machines en temps partagé, ne consiste pas seulement à taper des programmes dans un terminal et non dans une carte performée, mais d'encourager la communication proche."
Souvent présenté comme un héritage de CTSS, le système de temps partagé du laboratoire AI, UNIX tient aussi beaucoup d'ITS. Dans The UNIX-HATERS Handbook, Dennis Ritchie lui rendra hommage : *"Les systèmes dont vous vous rappelez avec tant d'affection (TOPS-20, ITS, Multics, Lisp Machine, Cedar/Mesa, the Dorado) ne sont pas que des rebuts, ils fertilisent en aval."* *[25]*
L'influence d'UNIX doit beaucoup à un décret de 1956 qui interdit à AT&T, propriétaire de Bell, de commercialiser des activités hors du domaine de la téléphonie. En revanche, AT&T pouvait tout à fait autoriser n'importe qui à utiliser ses produits, sur simple demande. Heureuse législation, puisque de nombreuses universités, entreprises et agences gouvernementales vont contribuer à son amélioration.
L'université de Berkeley en Californie développe la variante BSD qui engendrera plus ou moins directement plusieurs systèmes d'exploitation courants aujourd'hui, ce qu'on appelle la famille Unix, dont les plus connus du grand public sont Mac OS, et GNU/Linux et Android.
Si UNIX sera utilisé dans des versions commerciales, il remet en cause le business model d'alors, qui consistait à vendre un programme adapté à chaque machine, enchaînant le client : *"Les hackers UNIX se réjouissaient dans le sens qu'ils construisaient le futur en même temps qu'ils mettaient une chiquenaude au système*", résumera Eric S. Raymond dans *The art of UNIX programming*. Le futur, c'est entre autres Arpanet, l'ancêtre d'Internet, qui comblera cette aspiration à échanger entre communautés.

69, ANNÉE CONNECTÉE

"L'ordinateur comme outil de communication" et non simplement comme un moyen de faire des calculs, c'est cette vision totalement nouvelle des machines que le professeur JCR Lickider va pousser dans les années 60 à l'Arpa, et qui donnera l'Arpanet. Cette logique disruptive qui commence dans le sein de la recherche universitaire est alors à rebours de celle des entreprises :
"L'idée d'Arpa est que la promesse offerte par l'ordinateur comme moyen de communication entre les gens relègue à une insignifiance relative les débuts historiques de l'ordinateur en tant que machine à arithmétique." [26]
Ce qui relève de l'évidence aujourd'hui - faire communiquer n'importe quelles machines entre elles -, est alors un défi, qui nécessite d'inventer la manière dont elles vont communiquer, c'est-à-dire des

protocoles. Derrière leurs machines préférées, les PDP-10 de la marque DEC, qui sont les premières reliées au début, les hackers contribuent à l'essor de cet outil qui les enthousiasme en ouvrant des possibilités infinies d'échange. Issu du dictionnaire du TRMC qui a rassemblé le premier l'argot hacker, le fameux *Jargon files* circule d'ailleurs d'abord sur Arpanet. Le développement du réseau et de la communauté des hackers se nourrissent l'un l'autre. *"Les hackers de DP-10 s'emparèrent du fonctionnement d'Arpanet lui-même car personne d'autre ne voulait le faire,* raconte Eric S. Raymond. *Plus tard, ils formeront le cadre fondateur de l'Internet Engineering Task Force (IETF) et sont à l'origine de la standardisation par le biais de Requests For Comment (RFCs)."*
Alors qu'UNIX est en gestation, en 1969, Arpanet commence à fonctionner, timidement, en reliant quatre "noeuds" universitaires, les "Interface Message Processor" (IMP), des proto-routeurs. L'architecture d'Arpanet met en oeuvre l'idée de décentralisation en adoptant la transmission par paquets : les données sont découpées et peuvent du coup circuler par des voies différentes avant d'être reconstituées au final. Ce réseau est donc résilient, ce qui explique que les militaires financent le projet via Arpa : en cas d'attaque sur un des noeuds, la communication continue de passer par les autres points.
Le Network Working Group (NWG) réunit de façon assez informelle ces programmeurs pionniers issus de différentes universités, qui s'attellent à la mise en place des standards. Sous son sigle barbare, les Requests For Comment (RFCs) évoqués par Eric S. Raymond, représentent surtout une avancée majeure, mise en place en 1969 par Steve Crocker. Pour documenter les échanges, Steve Crocker propose d'en garder une trace sous forme de notes techniques, numérotées, sans prétention aucune :
"Je me souviens avoir eu très peur d'offenser les officiels de protocole, et j'ai passé une nuit à écrire des mots humbles pour nos notes. Les règles de base était que n'importe qui pouvait s'exprimer et que rien n'était officiel. Pour souligner ce point, j'ai qualifié ces notes de "Request for Comments." (littéralement "demande de commentaire", ndlr). *Je n'ai jamais rêvé que ces notes circulent à travers le véritable medium dont nous discutions dans ces notes. Discussions d'apprentis sorciers !"* [27]
Les modestes RFC vont en fait servir de base pour définir les contours sans cesse mouvants des spécifications techniques du réseau. Un succès tiré de son mode de fonctionnement, défini avec précision dans le troisième RFC. Le texte réaffirme la place centrale de l'ouverture, la participation et la collaboration plutôt que de la compétition et la bureaucratie :
"La documentation du travail du NWG se fait par des notes comme celle-ci. Les notes peuvent être produites sur n'importe quel site (universitaire, au sens de noeud du réseau, ndlr) et incluses dans cette série. [...] Ces standards (ou leur absence) sont spécifiés clairement pour deux raisons. D'abord, nous observons cette tendance à considérer les propositions écrites comme faisant autorité ipso facto. Notre but est plutôt d'encourager l'échange sur des idées pouvant être débattues. Deuxièment, il est naturel d'hésiter à publier une ébauche et nous espérons ainsi atténuer cette inhibition."
Face à la multiplication des initiatives, un protocole d'échange standard est développé et mis en place à partir de 1973, sous la houlette de Vinton Cerf et Robert Kahn : TCP/IP pour *Transmission* Control Protocol et Internet Protocol. Cela peut sembler un détail technique sans importance mais sur le fond, il illustre de nouveau ce que les hackers ont apporté à l'Internet : Arpanet choisit d'implémenter TCP/IP sur l'Unix version hacker ouverte BSD, et non sur la version propriétaire de l'entreprise DEC, par crainte qu'elle ne soit pas assez réactive pour modifier son logiciel[28]. La bascule sur TCP/IP est finie en 1983, la même année où Arpanet se scinde en deux. Sa partie militaire, Milnet, est séparée, tandis que les universités continuent de gérer Arpanet. Sans compter des jeunes gens très curieux...

Au Chaos Communication Camp. Création d'arcs électriques avec deux bobinesTesla. Dans les allées du campement, de nombreuses expériences prennent place, tout au long de la nuit. Allemagne, août 2011.

Espagne, Juillet 2011. À trois heures du matin, les conférences techniques s'enchaînent dans le petit Summer Camp de Garrotxa, au coeur des pyrénnées catalanes. Créé par Laura, aka Nusepas, en 2008, le campement accueille une trentaine de hackers dont la majorité sont issus du projet de WiFi communautaire, Guifinet.

Espagne, Juillet 2011. Moment de détente au milieu de la nuit sous les toiles de tente le petit Summer Camp de Garrotxa.
Deux hackers regardent des séries américaines, les ordinateurs toujours ouverts, connectés en WiFi, pendant que d'autres continuent de coder.

Chaos Communication Camp, août 2011. Projection de vieux épisodes de la série américaine de science-fiction, *Star Trek*, tard dans la nuit, à l'espace Baikonur. L'imagerie de la science-fiction a inspiré les décors de certains hackerspaces comme celui de C-Base à Berlin ou le Metalab de Vienne.

Chaos Communication Camp, août 2011. Le paradis des gamers se trouve sous la tente de l'"Awesome Retro Gaming Village". Des jeux rétros et une collection de consoles vieilles de vingt ans : *Commodores, Ataris, Segas*... On y trouve de tout, et particulièrement les jeux et consoles les plus anciens.

II. EN RÉSISTANCE

Les années 70 fleuraient bon la liberté, les années 80 sont celles de la réaction. “*Computing is serious business*” et les gamins qui se faufilent dans les réseaux et le principe de copie n’enchantent guère les gouvernements et les entreprises : le recadrage législatif était inévitable et marque le début d’une incompréhension profonde - d’une incompatibilité ? - entre deux logiques. La contre-culture hacker continue pourtant de s’épanouir et de s’organiser dans le cyberespace qui offre les outils de la mise en oeuvre de la libre circulation de l’information : ce sont les beaux jours des BBS, ces messageries où s’échangent des fichiers.

LES PETITS CONS EN PRISON

INTRUSIONS SANS PERMISSION

On n’est pas sérieux quand on a 17 ans, un ordinateur et un modem. L’image du jeune hacker surdoué doit beaucoup à une poignée de jeunes gens qui fichent la frousse à des organismes aussi prestigieux que le FBI ou des grosses entreprises, comme d’autres débrident leur pot de mobylette. Le terrain de jeu est nouveau, s’étend sans cesse par-delà les frontières, bref un bonheur à défricher pour un esprit curieux : puisque la porte est mal fermée, autant la pousser, non ?

Du haut de ses 17 ans, l’Américain Kevin Mitnick, alias Le Condor, se promène dans le central téléphonique de Pacific Bell à Los Angeles en 1980 et intercepte les lignes. En adepte des “pranks”, ces blagues potaches qu’affectionnent les hackers, il lui arrive parfois de répondre. Il s’amuse aussi à pénétrer dans la base qui répertorie les utilisateurs, une mine de données personnelles. Ces plaisanteries lui valent trois mois de prison. Il récidive en parvenant à se connecter à Arpanet en pénétrant un ordinateur du Pentagone. À l’époque, Arpanet est un réseau dont l’utilisation est réservée, et pas au premier venu : l’armée donc, les grandes universités, des administrations. Il prend six mois de prison cette fois-ci, qui auront un effet dissuasif tout aussi limité puisqu’il poursuivra ses exploits jusqu’en 1995 avant de se ranger des voitures.

Kevin Poulsen, aka Dark Dante, chatouille aussi Arpanet et se livre à une course-poursuite avec le FBI pendant 17 mois. Arrêté en 1991, il écope de la plus lourde peine infligée alors à un pirate informatique, quatre ans de prison, après un ultime coup mémorable : il remporte une Porsche offerte par une radio en étant le 102ème auditeur à appeler, comme le précisait le règlement. Faut-il préciser qu’il avait réussi à contrôler le standard de la radio ?

C’est aussi dans les années 80 qu’un des premiers vers est créé : Morris. Il doit son nom à Robert Tappan Morris, un étudiant de l’université américaine de Cornell qui lui donne jour en 1988. Le jeune homme n’a nullement l’intention de nuire : il souhaite connaître la taille du réseau Internet. Pour cela, il crée un programme qui se propage dans les systèmes Unix reliés à Internet en exploitant une faille du système d’exploitation. Parti du serveur Unix du MIT, le ver occasionne en fait des dégats dans 10% du réseau de l’époque, évalué à 60 000 connexions. Cela vaudra à Robert Tappan Morris d’être la première personne condamnée au nom du Computer fraud and abuse act. Face à la multiplication des intrusions, les Etats-Unis ont fait voter en 1986 une loi qui réprime le cracking des systèmes informatiques et les délits informatiques au niveau fédéral.

La coûteuse mésaventure - environ 100 000 dollars - a toutefois été fructueuse puisqu’elle fait prendre conscience à la communauté Internet de l’importance de mieux se prémunir contre les malwares : la DARPA met en place le premier Computer Emergency Response Team (CERT), qui sera ensuite dupliqué dans d’autres pays.

En France, la loi Godfrain de 1988 met fin au vide juridique. Souvenirs [29]du premier “pirate” français, Laurent Chemla, qui a eu l’audace de s’introduire dans le back office de Café Grand-Mère pour se créer une messagerie, si tant est que l’on puisse s’introduire dans une pièce grand ouverte :

“Informaticien programmeur, associé d’une toute petite société de services informatiques, j’ai toujours été passionné par les réseaux télématiques. Une passion qui m’a valu, en 1986, d’être le premier inculpé pour le piratage d’un ordinateur en France, piraté à partir d’un Minitel, certes, mais après tout, on a les gloires qu’on peut. Comme il n’existait pas encore de loi contre le piratage informatique, j’ai été inculpé de vol d’énergie. Tout cela s’est terminé par une relaxe mais, quand même, voilà de quoi lancer une belle carrière de voleur.”

Le voleur en question co-créera en 1999 Gandi, une société de gestion et administration de noms de domaine sur Internet, qui reversera une partie de ses bénéfices au projet alternatif Gitoyen, parce qu’il croyait *“à un Internet qui serait d’abord un outil citoyen avant d’être un système de vente à distance.”*

Sur le coup, du haut de sa petite vingtaine, le piratin s’amuse surtout, *“comme dans un jeu video dans lequel on cherche une solution à un problème, et dans lequel on accumule des “richesses” virtuelles”*, sans *“approche vraiment politique. Il y avait une conscience de nos actes, oui, et une sensation de liberté dans l’apprentissage et la découverte aussi.[30]”* Au même moment, de l’autre côté de l’Atlantique, un alter-ego écrit un texte fondateur, qui donne une autre dimension au piratage en éclairant son aspect politique : *La conscience d’un hacker*, ou *Le manifeste d’un hacker*.

LA CONSCIENCE D’UN HACKER

C’est un jeune homme de 21 ans qui a écrit ce court texte poétique en prison, en 1986, à la demande d’un ezine dédié au hacking, *Phrack*, qui deviendra ensuite une référence. Loyd Blankenship, connu sous le pseudo de The Mentor, a été condamné pour s’être livré aux joies du *phreaking*. Suivant avant l’heure les préceptes d’Eric S. Raymond, qui recommande aux hackers de lire de la science-fiction, Loyd a lu et apprécié The moon is a harsh mistress (*Révolte sur la Lune*) : *“J’ai sans doute été très influencé alors par ce livre”*, explique-t-il.

Ce roman de science-fiction, écrit en 1966 par l’Américain Robert A. Heinlein, raconte la révolte en 2076 d’une ancienne colonie pénitentiaire basée sur la Lune contre l’Autorité qui la contrôle depuis la Terre. Parmi les personnages principaux, Mannie Davis, un informaticien rebelle en charge de Mike, un superordinateur de l’Autorité lunaire qui acquiert la conscience. Une œuvre très politique donc, imprégnée de la pensée libertarienne auquel le texte de Loyd fait effectivement écho, en la mâtinant d’échos rimbaldiens, révolte adolescente oblige. Le hacker se décrit comme un enfant surdoué rejeté par un monde technocratique anonymisant et policé, en proie au capitalisme sauvage, et qui l’ennuie.

“Un autre a été pris aujourd’hui, c’est dans tous les journaux. ‘Un adolescent arrêté dans un scandale de crime informatique.’ ‘Arrestation d’un Hacker après des tripatouillages bancaires.’ Saleté de gosses. Tous pareils. Mais vous, dans votre psychologie trois-pièces et dans votre technocervelle des années 50, avez-vous jamais regardé derrière les yeux du hacker ? Est-ce que vous vous êtes jamais demandé ce qui le déclenche, quelles forces lui ont donné forme, qu’est-ce qui a bien pu le modeler ? Je suis un hacker, entrez dans mon monde...”

C’est dans l’informatique qu’il trouve une échappatoire, plus encore, un outil à même de satisfaire ses aspirations, et en particulier d’étancher sa soif de connaissance - *“une porte s’est ouverte sur un monde... “* - Et pour cela, il entend bien l’explorer en toute liberté.

Là où la société dénonce des criminels tout juste bons à envoyer en prison, lui ne voit que de la curiosité et une façon d’échapper à ce qu’il considère comme un racket. Un quart de siècle plus tard, ce même argument est avancé par les internautes qui s’opposent à la répression du téléchargement illégal : *“Nous utilisons un service déjà existant sans payer pour ce qui pourrait valoir des clopinettes si ce n’était pas administré par des gloutons profiteurs, et vous nous traitez de criminels. Nous explorons... et vous nous traitez de criminels. Nous cherchons le savoir... et vous nous traitez de criminels.”*

C’est dans l’informatique qu’il trouve une échappatoire, plus encore, un outil à même de satisfaire ses aspirations, et en particulier d’étancher sa soif de connaissance - *“une porte s’est ouverte sur un monde...”* - Et pour cela, il entend bien l’explorer en toute liberté.

Là où la société dénonce des criminels tout juste bons à envoyer en prison, lui ne voit que de la curiosité et une façon d'échapper à ce qu'il considère comme un racket. Un quart de siècle plus tard, ce même argument est avancé par les internautes qui s'opposent à la répression du téléchargement illégal : *"Nous utilisons un service déjà existant sans payer pour ce qui pourrait valoir des clopinettes si ce n'était pas administré par des gloutons profiteurs, et vous nous traitez de criminels. Nous explorons... et vous nous traitez de criminels. Nous cherchons le savoir... et vous nous traitez de criminels."*
Quant aux deux derniers vers, ils anticipent les légions des Anonymous, le collectif informel d'hacktivistes qui déstabilise gouvernements et majors de l'industrie culturelle avec ses attaques imprévisibles contre leurs sites et son caractère insaisissable [31] :
"Vous pouvez arrêter cet individu, mais vous ne pouvez pas tous nous arrêter... après tout, nous sommes tous les mêmes."
Cette conscience politique commence à s'incarner dans d'autres collectifs qui esquissent les prémisses de l'hacktivisme. Aux Etats-Unis, la crème des hackers qui échangent sur les BBS forment en 1984 The cult of the deadcow (cDc, "le culte de la vache morte"), et choisit pour lieu de réunion... un abattoir abandonné du Texas, sous la houlette de "Grandmaster Ratte", "Franken Gibe" et "Sid Vicious". À la fois collectif et média, doté d'un sens certain de l'auto-dérision, à l'image de son délicieux petit nom, the cDc affiche comme objectif *"la domination globale à travers la saturation des médias"*.
Les membres jouent de leur image de "bad guys", quitte à passer pour des satanistes ou des criminels. *"Cela n'a pas aidé que les boards de hackers underground arborent des noms terrifiants de science-fiction heavy metal, comme 'Speed Demon Elite', 'Demon Roach Underground', et 'Black Ice'"*, notera Bruce Sterling dans son ouvrage sur la répression contre les hackers,*The Hacker crackdown[32]*. The cDc se fiche de l'opinion des puritains de tous poils, et derrière ce décorum underground, devient une des références mondiales en matière de sécurité informatique et de réflexion sur le rôle des technologies.
Ils sont aussi à l'origine, en 1990, de la première grosse convention de hackers, HoHocon, où sont aussi conviées les forces de l'ordre. Le concept rendra par la suite bien service aux gouvernements : les hackers farceurs finissent parfois par travailler dans la sécurité et les conférences de hackers les plus réputées comme DefCon ou le Chaos Computer Congress servent de lieu de recrutement pour les entreprises et les administrations... Et dès les années 80, les Etats-Unis, l'Allemagne ou encore l'URSS ont déjà bien compris l'intérêt de recourir aux hackers. Car derrière le jeu et la curiosité, ces aventuriers insolents posent les bases de la sécurité informatique : intrusion, faille de sécurité, base de données personnelles, malwares, les entreprises et gouvernements sont prévenus : ils vont devoir prendre au sérieux la sécurité informatique. Pour reprendre la jolie expression de Ralf Bendrath, conseiller politique de l'eurodéputé Vert Jan Philipp Albrecht et ancien hacker, *"nous avons besoin des hackers car ils servent de système immunitaire de la société de l'information."*

GUERRE ET PRIVACY[33]

Suspect aussi le goût de certains hackers pour le "secret", anonymat et cryptographie. Il faut dire qu'à cette époque, cette dernière est classée dans la catégorie des armes de guerre, au même titre qu'un char d'assaut ou une bombe atomique. C'est une science cultivée dans le secret par les militaires. Dans les années 70, elle sort un peu de l'ombre avec la mise en place du Data Encryption Standard (DES) par IBM avec le soutien du gouvernement américain, à destination des banques. Les échanges dématérialisés commencent en effet à se développer et il faut sécuriser les systèmes. Toutefois, le chiffrement reste strictement encadré : hors de question que le grand public s'en serve.
Les fers de lance les plus virulents de la cryptographie sont les hackers du mouvement cypherpunk, qui émerge à la fin des années 80. Leur but : mettre la cryptographie au service de la cause anarchiste, comme leur nom le suggère : cypher, chiffrer en anglais et punk, comme les jeunes gens qui *shockaient* la reine d'Angleterre dans les années 70's à grand coup de *Anarchy in the UK*. Et une référence au cyberpunk, le courant de science-fiction dystopique popularisé par le roman de William Gibson, *Neuromancien* en

1984. Pour la petite histoire, ce mot-valise a été inventé par Jude Milhon, une hackeuse qui traînait déjà ses lignes de code dans les communautés des années 70, en comparaison de laquelle les geekettes avec leurs iPhone roses sont de fades avatars.
Leur discours, empreint d'idéologie libertarienne, pose la cryptographie comme un droit inaliénable, et tant pis si cela sert aussi à des criminels. Qu'on partage ou non leur idéologie, leur antienne sonne plus que jamais d'actualité, à l'heure où la surveillance des réseaux est devenue un business aussi amoral que juteux qui fait le lit des dictatures : les cypherpunks ont tout simplement senti l'importance de défendre la privacy avec l'avènement de la société de l'information : *"Cypherpunks du monde, la technologie informatique est sur le point de fournir aux individus et aux groupes la possibilité de communiquer et d'interagir les uns avec les autres d'une manière totalement anonyme."* [34]
"À l'ère électronique, la "privacy" est une nécessité pour toute société ouverte. Cette notion de "privacy" est différente de la notion de secret. Une affaire est privée lorsque la personne concernée ne veut pas en parler au monde entier, mais une affaire est secrète lorsqu'elle ne doit être révélée à personne. La "privacy" est le pouvoir de se révéler soi-même au monde de manière sélective." [35]
Ce faisant, ils ont aussi anticipé avec acuité l'argumentaire anti-chiffrement en affirmant que *"l'Etat essaiera bien sûr de ralentir ou d'arrêter la diffusion de cette technologie, en invoquant les nécessités de la sécurité nationale, l'utilisation de la technologie pour le trafic de drogue et l'évasion fiscale, et des craintes de désintégration sociétale."* [36]
Les cypherpunks remettent aussi en cause la légitimité de la notion de propriété intellectuelle en tissant la métaphore du nouveau Far West que représente le "cyberespace", comme on l'appelait alors :
"Et tout comme une invention apparemment mineure comme le fil de fer barbelé a rendu possible la clôture de vastes fermes et ranchs, altérant ainsi pour toujours les concepts de terre et de droits de propriété dans l'Ouest de la Frontière, la découverte apparemment mineure venue d'une obscure branche des mathématiques deviendra les pinces coupantes qui démantèleront le fil de fer barbelé qui entoure la propriété intellectuelle. Debout, tu n'as rien d'autre à perdre que tes clôtures de barbelé !"
En 1991, un logiciel libre et gratuit du nom de PGP viendra démocratiser le chiffrement. Mais la justice, on le verra plus loin, entravera encore pendant quelques temps la libéralisation des outils de chiffrement[37].
La conscience politique des hackers va aussi se structurer à travers deux organisations encore très actives aujourd'hui, qui prennent la voie d'un lobbying plus classique, avec pignon sur rue. Il y a l'idée que la loi est un système comme un autre et qu'à ce titre, elle peut être hackée, débugguée.

HACKER LA LOI

LE CHAOS COMPUTER CLUB

Le premier lobby hacker naît au début des années 80 à Hambourg en Allemagne de l'Ouest, et l'histoire du pays n'y est pas étrangère. Andy Müller-Maguhn, qui l'a rejoint en 1985 et fut longtemps son porte-parole, se souvient :
"Le Chaos Computer Club (CCC) a été créé de façon informelle en 1981, par des pros de l'informatique qui se réunissaient pour discuter de l'impact des outils informatiques et de leur utilisation sur la société en tant que tel. Ils avaient dressé une liste des problématiques comme la privacy. Des questions comme celle de la vie privée sont très sensibles, notamment avec l'histoire de l'Allemagne de l'Est. On sait à quel point les abus structurels sont dangereux, parce que nous sommes passés par là, notamment en mettant des étoiles jaunes sur des gens avant de les envoyer à la mort. Donc nous sommes aux aguets mais cela vient aussi du système éducatif allemand : à l'école, vous apprenez l'histoire du nazisme. Les Allemands sont anti-autoritaires. Vous ne trouverez personne ici pour vous donner un ordre."
Le CCC s'est constitué plus officiellement en 1984, avec la sortie de leur magazine *Die Datenschleuder*

(*L'essoreuse à données*, littéralement, ndlr), qui *"éclaire aussi bien sur les possibilités existantes que sur les dangers"*, et le premier Chaos Communication Congress, une conférence annuelle devenue au fil du temps incontournable par la qualité de ses intervenants.
Très vite, le CCC effectue un véritable travail de pédagogie auprès des pouvoirs. Une pédagogie pas toujours très orthodoxe qui leur vaudra quelques ennuis... Il entre dans les annales en 1984 avec leur premier fait d'arme, le hack du Bildschirmtext, le Minitel allemand. Ils choisissent de démontrer avec un test grandeur nature que ce nouvel outil vanté par la Poste allemande comme un moyen de paiement fiable est en réalité troué comme une passoire : ils dérobent 134 000 DM à une banque de Hambourg avant de les remettre le lendemain. La démonstration ne sera guère appréciée :
"Notre démarche a été mal interprétée par les hautes sphères gouvernementales, qui se demandaient si nos activités n'étaient pas criminelles. Donc bien sûr il y avait des enquêtes, tout un mic-mac autour de nous. C'est ce que font les gouvernements s'ils ressentent le besoin de reprendre le contrôle." [38]
En Allemagne, le contexte est particulièrement porteur pour le CCC : les années 80 sont marquées par des protestations très fortes contre un projet de recensement de la population, accusé de présenter des risques sur la sécurité des données collectées. Le gouvernement finit par reculer face à l'ampleur de la contestation, le texte initial sera retoqué par la Cour constitutionnelle. 20 ans plus tard, ils poseront de nouveau avec fracas le débat sur la table en démontrant que la carte d'identité biométrique n'est pas fiable, empreinte digitale du ministre de l'Intérieur à l'appui.
Conscient que la frontière entre le blanc et le gris est ténue, le CCC apprend aussi à s'entourer : *"Dans les années 80, peu de gens comprenaient ce qu'on faisait"*, se rappelle Andy Müller-Maguhn, *"c'était une vraie sous-culture, nous avions pas mal de problèmes juridiques, et nous avons dû nous renforcer sur ce point avec des experts. Que pouvions-nous hacker ou pas ? Comment faire la distinction entre ce qui est légal et les activités grises ?"*
Si certains hackers du CCC iront se fourvoyer dans des affaires d'espionnage qui feront quelques cadavres[39], cette solide base mise en place leur permet d'acquérir un véritable poids :
"le CCC est une entité acceptée et reconnue parce qu'elle fait un travail pédagogique sur les technologies auprès du public depuis les années 1980, poursuit Andy Müller-Maguhn. Nous avons toujours eu des histoires étranges qui nous parvenaient, sur des données qui disparaissent par exemple, et que nous pouvions expliquer. Les médias allemands nous ont toujours perçus comme des gens qui savent vraiment ce que sont les technologies, leurs avantages et les dangers, et pas pour des types qui travaillent pour des entreprises ayant des intérêts économiques. Nous avions donc le pouvoir de la définition et nous l'avons toujours utilisé."
En France malheureusement, aucun équivalent n'a pu éclore après l'affaire du Chaos Computer Club de France. Cette pâle copie est créée à Lyon en 1988 par Jean-Bernard Condat, un étudiant téléguidé par la DST qui espère grâce à ce sous-marin surveiller les activités de ce milieu hacker à l'image "sulfureuse". Et éventuellement recruter en forçant quelque peu la main : un hacker pris en train de commettre des infractions était invité à coopérer gentiment en échange d'un coup d'éponge. Un chantage souvent efficace sur des jeunes gens. L'épisode serait resté aux oubliettes s'il n'avait eu pour funeste conséquence de jeter l'opprobre sur le terme hacker en France pendant plus d'un quart de siècle. La communauté se regroupera sous le vocable rassurant de "défenseur du logiciel libre".

EN DÉFENSE DU FAR WEST

Pendant que les services de renseignement français se livrent à leurs petites manipulations, les hackers américains ouvrent eux aussi une page de l'histoire de leur activisme en créant l'Electronic Frontier Foundation (EFF) en juillet 1990 *"en réponse à une menace fondamentale sur la liberté d'expression"*. Selon le récit qu'en fait John Perry Barlow, un des fondateurs de l'EFF, une visite malencontreuse du FBI est à l'origine de tout. Un agent de l'agence de renseignement américaine vient interroger celui qui est

alors encore parolier du groupe culte The Grateful Dead et arpenteur averti du cyberespace, sur son appartenance supposée à Nu Prometheus League, un groupe qui a revendiqué le vol et la distribution de code source d'Apple. Son interlocuteur est frappé par sa crasse ignorance technique qui mine la possibilité que la vérité fasse jour :
"La mission de l'agent Baxter s'est compliquée à cause de sa méconnaissance quasi-totale de la technologie informatique. J'ai réalisé tout de suite qu'avant de pouvoir prouver mon innocence, il allait d'abord falloir que je lui explique ce que la culpabilité pouvait être. Les trois heures que j'ai passées à faire ça ont été surréalistes, pour lui comme pour moi."
Il évoque l'entretien sur une des plus anciennes communautés virtuelles, Whole Earth 'Lectronic Link, aka The WELL, co-créée par Stewart Brand, l'homme de The Whole Earth Catalog, où les technophiles éclairés ont l'habitude de se croiser. Avec deux d'entre eux, ils décident de former un groupe pour *"travailler sur les sujets liés aux libertés publiques soulevés par les nouvelles technologies"* : Mitch Kapor, le très riche fondateur de Lotus et John Gilmore, un ancien de Sun, cypherpunk émérite, qui lui aligne tout de suite un chèque à six zéros. Steve Wozniak, qui a quitté Apple cinq ans auparavant, fait partie de leurs soutiens de la première heure.
Très vite, l'Electronic Frontier Foundation entre dans le dur, en apportant son soutien à un éditeur de jeux de cartes et de rôles, Steve Jackson. La source de ses ennuis judiciaires vient d'un document piraté en 1988 sur un ordinateur de l'entreprise de télécommunication Bellsouth par un membre de *Phrack*. Il est publié l'année suivante dans le fameux e-zine underground : le mode d'emploi de l'équivalent américain du 112, le 911. Panique : *"Les services secrets pensaient que si des 'hackers' savaient utiliser les lignes pour les appels d'urgence, elles seraient saturées et les gens confrontés à de véritables urgences ne pourraient pas y accéder."*
Soupçonné à tort d'avoir obtenu une copie, Steve Jackson voit ses ordinateurs saisis et sa maison d'édition mise en péril. Et quand il les récupère, il a la mauvaise surprise de constater avec ses employés que le FBI est non seulement allé fouiner dans leurs échanges électroniques stockés sur leurs BBS, mais qu'en plus, il les a effacés. Furieux, il souhaite se retourner contre l'Etat mais ne trouve personne pour l'assister. Personne excepté la toute nouvelle EFF.
Le geste de Phrack fera partie des éléments déclencheurs d'une opération d'envergure nationale contre le piratage des cartes de crédit et le *phreaking* : l'opération Sundevil, menée de 1988 à 1990. Il s'agit de frapper les esprits à grands coups de saisies de disques durs, de BBS et d'ordinateurs. Et de rassurer les entreprises concernées. *Phrack* se désole que tout le monde soit mis dans le même sac : *"c'est mon sentiment que [l'assistante de l'attorney general (ndlr : le ministre de la Justice américain)] et les services secrets ne prennent pas cela à la légère. Elle a déclaré à Phrack inc. qu'ils ne font pas de différence entre pirates, hackers et phreakers. En gros, c'est n'importe quel gamin avec un modem qui appelle avec un alias. Oui, nous sommes les sorcières et nous allons être chassés."*
Chassées mais fûtées, les sorcières de *Phrack* font un pied de nez à la justice avec l'aide de l'EFF : lors de son procès, elles lui fournissent un témoin qui explique que Bell vendait ledit mode d'emploi pour 13 dollars : s'il avait bien été pris illégalement sur un ordinateur de la firme, il n'avait en revanche aucune utilité.
L'économie numérique devra beaucoup à ses sorcières, ce que reconnaissent en substance les services secrets dans un communiqué de presse publié dans la foulée de l'opération :
"La 'privacy' de nos citoyens et la santé de notre économie dépendent de systèmes informations sécurisés et fiables."
Les réseaux informatiques sont une passoire et les hackers servent à montrer les trous et donc à améliorer le réseau. En ces années 80 placées sous le signe du logiciel propriétaire, certains rappellent aussi, avec fracas, l'importance de laisser le code ouvert.

Londres, novembre 2011. Le grand rassemblement annuel de la fondation Mozilla. Elle milite activement pour le développement des logiciels libres et un web libre et ouvert (*Open Web*). Cette deuxième édition était axée sur les médias et le journalisme de données. La première édition, dédiée au D.I.Y, avait eu lieu à Barcelone en 2010.

Les hackers rencontrent les journalistes et les ONG : Okhin, agent du groupe informel de hackersTelecomix, pendant son atelier sur la sécurisation de la navigation web. Une journée d'ateliers organisée à La Cantine à Paris, en février 2011.

LIBRE !

GRANDEUR ET DÉCADENCE DU LABORATOIRE D'AI DU MIT

Richard Stallman, aka rms : *"le dernier des hackers, qui s'est voué à la défense des principes du hackerism, jusqu'à la toute dernière fin."* Steven Levy n'a pas de mots assez laudatifs pour décrire le père du logiciel libre, gourou barbu entouré de ses fidèles adeptes, sectaire disent certains. Précisons qu'il lui attribue ce qualificatif en 1984 et que depuis, le relai est assuré.

Avant de devenir un symbole de la résistance au logiciel propriétaire, ce hacker américain a commencé à travailler dans le laboratoire AI du MIT dans les années 70. Il s'est fait connaître en travaillant sur Emacs, un éditeur de code en LISP très évolutif et multiforme, un outil de hacker par excellence : il est fait pour que l'utilisateur l'adapte à ses besoins, à condition qu'il maîtrise LISP. Débutants en BASIC, s'abstenir.

Au début des années 80, il claquera pourtant la porte du lab pour initier un mouvement majeure de l'histoire de l'informatique, le logiciel libre. La suite logique du contexte à la fois général et personnel. Comme nous l'avons déjà évoqué dans le chapitre précédent, la deuxième moitié des années 70 marque la fin du paradis originel des hackers. L'entreprise hacker a fait long feu et les petits Bill Gates se multiplient. Progressivement, le prix des machines baisse grâce aux progrès de la micro-informatique et au développement de systèmes d'exploitation standards, le capot des machines se referme, le prix de la démocratisation du "personal computer", le PC. Le logiciel devient au centre du business model, vendu en pack avec les machines.

Version storytelling "la légende dorée de rms", il y a la sempiternelle anecdote du bourrage papier d'une banale photocopieuse à l'origine de sa prise de conscience du danger du logiciel propriétaire. Le laboratoire disposait d'une imprimante Xerox dont le code source était disponible, ce qui permettait aux

hackers de la bidouiller selon leurs besoins. Au début des années 80, une nouvelle imprimante arrive au lab. Confronté à des bourrages-papier récurrents, Stallman ouvre le capot, constate à sa grande surprise qu'il n'y a pas le code source. Il demande donc à l'entreprise qui la fabrique le code source pour corriger ce bug. La réponse le met en rage : il peut accéder au code source à condition de signer un accord de non-divulgation. Ce qu'il refuse, vous vous en doutez.
Moins folklorique, le laboratoire d'AI est petit à petit vidé de ses hackers, qui commencent eux aussi à mettre des dollars dans leur éthique. Ils travaillent alors à un projet de machine conçue pour le LISP, sous la houlette principalement de Richard Greenblatt. Le projet attire des commandes, ouvrant la perspective d'un nouveau marché. Deux sociétés concurrentes naissent alors ; l'une, Symbolics, pensait surtout gros sous alors que l'autre, Lisp Machines Inc. à l'iniative de Greenblatt, se revendique de l'éthique hacker. Persuadée à tort que son rival échouera, Symbolics débauche une majorité des hackers du laboratoire. Par accord de principe, les deux sociétés reversent le code source au MIT. Symbolics estime que cela relève de la concurrence déloyale puisque que son rival bénéficie ainsi des avancées de sa grosse équipe. Il décide donc de mettre fin à l'accord.
Au milieu du gué, Richard Stallman, en irréductible barbu isolé, refuse de rejoindre le privé et continue seul de mettre à jour le code source de la machine LISP du laboratoire, malgré l'obstruction de Symbolics. Un véritable exploit passé à la postérité, qui lui vaut le respect de tous.
Le dernier élément déclencheur est juridique : en 1983, sous le coup d'un procès anti-trust, AT&T parvient à un accord avec le gouvernement américain et se sépare de ses filiales Bell régionales en échange d'une levée des restrictions du décret de 1956. La compagnie peut donc enfin commercialiser sa version d'UNIX[40].

LÂCHER DE GNU

Au début des années 80, Richard Stallman apparaît de plus en plus comme une survivance inexplicable et même dangereuse :
"Ignorant tout de la culture hacker et de son aversion pour le logiciel pré-compilé, la plupart des utilisateurs n'éprouvèrent pas le besoin de protester lorsque ces compagnies cessèrent de fournir leurs programmes accompagnés des fichiers contenant le code source. [...] Au tournant des années 1980, la vente de programmes ne constituait plus seulement un moyen d'amortir les coûts : c'était devenu un enjeu politique. À l'heure où l'administration Reagan s'empressait de démanteler nombre de règlements fédéraux et suspendait les projets publics échafaudés durant le demi-siècle qui avait fait suite à la Grande Dépression, plus d'un programmeur considérait l'éthique des hackers comme anti-compétitive et, par extension, anti-patriotique. Au mieux, c'était un retour aux attitudes anti-corporatistes de la fin des années 1960 et du début des années 1970. Tel un banquier de Wall Street découvrant un de ses vieux T-shirts hippies caché entre ses chemises Cardin et ses costumes trois-pièces, nombre d'informaticiens ne regardaient plus l'éthique des hackers que comme le rappel embarrassant d'une époque idéaliste." [41]
Tous ces éléments conduisent Richard Stallman à démissionner du MIT en 1984 pour développer GNU (pour GNU N'est pas UNIX), une alternative libre à Unix, avec fracas et panache, orgueil si l'on se situe dans le camp de ses détracteurs : *"Plutôt que de passer sa vie à châtier ceux qui avaient détruit son ancienne communauté, Stallman préféra en fonder une nouvelle."[42]*
Dans *Le manifeste GNU* de 1985, il grave les raisons de son choix, réaffirmant la dimension profondément éthique du logiciel libre :
"Dans mon opinion, la Règle d'or veut que, si j'apprécie un programme, je dois le partager avec d'autres qui apprécient ce programme. Les éditeurs de logiciels cherchent à diviser et à conquérir les utilisateurs, en interdisant à chacun de partager avec les autres. Je refuse de rompre la solidarité avec les autres utilisateurs de cette manière. Je ne peux pas, en mon âme et conscience, signer un accord de non-divulgation ou une licence de logiciels. Pendant des années, j'ai œuvré au sein du

Laboratoire d'intelligence artificielle du MIT pour résister à ces tendances, mais finalement, ils sont allés trop loin : je ne pouvais pas rester dans une institution où de telles choses avaient lieu contre ma volonté.
Pour pouvoir continuer à utiliser les ordinateurs en accord avec ma conscience, j'ai décidé de rassembler un ensemble suffisant de logiciels libres, pour pouvoir me débrouiller sans logiciels non libres. J'ai démissionné du laboratoire d'intelligence artificielle pour que le MIT ne puisse invoquer toutes les excuses légales pour m'empêcher de distribuer GNU librement."
Un logiciel libre doit respecter quatre libertés fondamentales : l'utilisateur peut l'exécuter, l'étudier, le modifier et redistribuer les versions modifiées, ce qui implique que les modifications apportées au code source doivent être redistribuées à la communauté. Plus qu'un simple outil technique, le logiciel libre s'apparente à une philosophie que Stallman résume "en trois mots : liberté, égalité, fraternité… "
La même année, la Free Software Foundation est créée pour prendre en charge le développement de GNU. La licence publique générale (GPL) élaborée par le juriste Eben Moglen est publiée en 1989 pour donner un cadre légal et pérenniser les idéaux du logiciel libre. Cette dimension éthique n'est pas incompatible avec la notion d'argent : on pense souvent à tort que le libre signifie gratuit en raison du double sens de "free" en anglais, qui signifie à la fois libre et gratuit. Ainsi dès 1989, John Gilmore crée avec deux associés Cygnus solutions, dont le business model repose sur la fourniture de support autour du logiciel libre. Avec le temps, cette économie se développera et se diversifiera.

CCCamp, août 2011. A l'espace Kourou, conférence *Cyberpeace & Datalove* par Jérémie Zimmermann, porte parole de La Quadrature du Net, association de défense des libertés sur Internet. *"Au nom d'une 'cyberwar' à venir, les gouvernements pourraient parvenir à contrôler le réseau et restreindre nos libertés. (...) Mais qu'est-ce que cette 'cyberwar' ?"*

Paris, mai 2011. Au sommet de l'e-G8, John Perry Barlow, co-fondateur de l'Electronic Frontier Foundation, est l'invité surprise de la discussion sur *"la propriété intellectuelle et l'économie de la culture à l'heure du digital"*. Entouré d'Antoine Gallimard, Pascal Nègre (président d'Universal), le patron de la Twentieth Century Fox, celui de Bertelsmann et de Frédéric Mitterrand, alors ministre de la Culture, le débat tourne vite à la foire d'empoigne. Tandis que Pascal Nègre défendait son fonds de commerce en affirmant que le Net *"crée des déserts culturels"*, Barlow répondait par un soupir: "Mon Dieu, je ne vis pas sur la même planète".

Richard Stallman, fondateur de GNU et de la Free Software Foundation lors de sa venue à Paris en juin 2012 pour une conférence sur les logiciels libres et les droits de l'homme, organisée avec la FIDH et RSF.

Paris, place des Victoires, février 2012. Fin de la manifestation contre ACTA (Accord commercial anti-contrefaçon), à l'initiative de La Quadrature du Net.

Paris, juin 2012. Au festival hacker Pas Sage en Seine, conférence de Benjamin Bayart, président et co-fondateur du plus vieux fournisseur d'accès associatif à Internet FDN (French Data Network). Modèle alternatif aux géants des Télécoms, le réseau FDN défend la neutralité du net, et s'oppose à ACTA. Les conférences comme "Internet, Minitel 2.0" sont devenues cultes.

III. INTERNET, TERRAIN DE BATAILLE GRAND PUBLIC

www pour World Wide Web : au début des années 90, le vieux rêve du village mondial connecté devient réalité. Le concept de la Toile, pour reprendre l'expression un peu désuète, naît en 1989 quand Tim Berners-Lee[43], un informaticien du Cern, l'organisation européenne pour la recherche nucléaire, propose de combiner le concept d'Internet, un protocole d'échanges de données en réseau par paquet, avec celui de l'hypertexte pour faciliter l'échange d'informations entre les chercheurs. Heureusement, l'idée sort du Cern pour constituer petit à petit le web tel que nous le connaissons. Avec le développement des navigateurs, le grand public s'approprie cet espace qui croît à grande vitesse et le web devient vite l'objet de toutes les convoitises lucratives.

Tout le web ? Non, car quelques irréductibles hackers résistent, aux côtés de l'ancienne génération. Cette nouvelle cohorte a grandi avec le PC et Internet, et entend tout naturellement exploiter les possibilités de partage sans précédent qu'elle offre : ce serait dommage d'en rester aux échanges de cassette de la main à la main...

L'Internet n'est pas qu'un moyen de pousser plus loin les idéaux du partage de la culture. Grâce à lui, le logiciel libre va aussi prendre un nouveau souffle qui ne s'est pas démenti depuis.

LIBRES SOUS TOUTES SES FORMES

L'OS QUI VENAIT DU FROID

Le 25 août 1991, un étudiant en informatique finlandais laisse un message sur Usenet qui fera date dans l'histoire de l'informatique :

"Bonjour à vous qui utilisez minix - Je suis en train de créer un système d'exploitation (gratuit) (et c'est juste un passe-temps, ça ne sera pas aussi énorme et professionnel que GNU) pour 386 (486) clones du modèle AT d'IBM. C'est sur le feu depuis avril, et ça commence à prendre forme. J'aimerais bien avoir un retour sur ce que vous aimez / n'aimez pas avec minix, puisque mon OS lui ressemble d'une certaine manière (par exemple, la présentation pour le système de fichiers est la même (pour des raisons pratiques))."

Traduction de ce jargon : Linus Torvald, notre étudiant, demande de l'aide pour son nouveau projet, un système d'exploitation basé sur MINIX. MINIX est un système d'exploitation simplifié, basé sur UNIX mais dont le code est libre. En effet, son créateur, le professeur Andrew S. Tanenbaum s'en sert pour apprendre à ses élèves les bases d'un OS et UNIX est, souvenez-vous, propriétaire depuis 1983. Mais il n'est pas modifiable, ce qui frustre l'étudiant et le motive à développer un OS complètement libre[44].

Rétrospectivement, l'annonce de Linus Torvald prête aussi à sourire : le petit loisir est devenu un pilier de la culture hacker et a contribué un peu plus à rééquilibrer la balance avec les OS propriétaires. Au début des années 90, l'objectif de Richard Stallman est en effet loin d'être atteint puisque les contributeurs n'ont pas réussi à développer un noyau entier et le projet patine dans une ambiance qui se dégrade. GNU est du coup resté une alternative utilisée par des utilisateurs très avertis ; quant au grand public, il ne se pose même pas la question et se sert d'OS propriétaires, MS-DOS, Mac OS 2 ou Windows. A contrario, Linux connaît un succès rapide et imprévu avec une communauté estimée fin 93 entre 20 000 et 100 000 personnes[45]. Avec l'appui du réseau ouvert de contributeurs constitués grâce à Internet, Linux a grandi vite et plutôt bien. Vite mais aussi de façon désordonnée avec des distributions commerciales qui poussent à droite à gauche sans respecter toujours la licence GPL et d'une qualité inégale.

Alors quand Ian Murdock, un étudiant en informatique, propose de développer une distribution fusionnant GNU et Linux, Richard Stallman donne son saint aval. Soutenu par la Free Software Foundation, Debian

sort en août 1993 et c'est aujourd'hui encore une des principales distributions[46].
Autour de GNU/Linux, des sociétés vont se développer à destination des entreprises pour qui le choix du libre constitue une alternative intéressante financièrement, comme Red Hat, une des belles réussites du secteur. Il faut dire que Linus Torvald, contrairement à Richard Stallman, a une vision moins binaire des choses, tout codeur qu'il soit. Très vite, il devient la figure de proue de la jeune génération de hackers qui place l'efficacité avant le respect des valeurs. Son approche plus souple - moins éthique soupirent les adeptes de Stallman - encourage le développement de l'économie du libre :
"Je suis généralement assez pragmatique : ce qui fonctionne, fonctionne. En matière de logiciels, je préfère de loin le logiciel libre, car j'ai rarement rencontré un programme qui remplisse tous mes besoins, et disposer du code source peut sauver la mise. [...] Cependant, cela ne signifie pas que je suis opposé au logiciel commercial. Le développement de logiciels commerciaux a lui aussi certains avantages — les aspects lucratifs introduisent de nouvelles motivations, absentes pour la plupart des logiciels libres. Et ces motivations ont souvent pour effet de produire un logiciel plus fini.[47]"
Il est en cela proche d'Eric S. Raymond, qui provoque une scission au sein de la Free Software Foundation à la fin des années 90 en proposant une vision du libre orientée business et non philosophie.

ET L'ARGENT COULE DE SOURCE

Eric S. Raymond est un hacker américain d'une espèce bien particulière : libertarien pur et dur, il prône la liberté totale, y compris celle de porter des armes. Il a observé avec grand intérêt le mode de fonctionnement disruptif initié par Linus Torvald, qu'il théorise en 1997 dans un essai devenu célèbre, *La cathédrale et le bazar* :
"J'analyse le succès d'un projet de logiciel dont le code source est ouvert, fetchmail ("va chercher le courrier'"), qui a été lancé délibérément pour tester certaines théories surprenantes du génie logiciel suggérées par l'histoire de Linux. Je discute ces théories en termes de deux styles de développement fondamentalement différents, le modèle "cathédrale" de la majorité du monde commercial, à opposer au modèle "bazar" du monde de Linux." [...] "Linux est subversif. Qui aurait imaginé, il y a seulement cinq ans, qu'un système d'exploitation de classe internationale prendrait forme comme par magie à partir de bidouilles faites pendant le temps libre de plusieurs milliers de développeurs disséminés de par le monde, et reliés seulement par les liens ténus de l'Internet ?" [...] "Le style de développement de Linus Torvalds - distribuez vite et souvent, déléguez tout ce que vous pouvez déléguer, soyez ouvert jusqu'à la promiscuité - est venu comme une surprise. À l'opposé de la construction de cathédrales, silencieuse et pleine de vénération, la communauté Linux paraissaît plutôt ressembler à un bazar, grouillant de rituels et d'approches différentes (très justement symbolisé par les sites d'archives de Linux, qui acceptaient des contributions de n'importe qui) à partir duquel un système stable et cohérent ne pourrait apparemment émerger que par une succession de miracles."
Si l'invention de ce nouveau modèle de développement ne saurait être attribué entièrement à Linus Torvald, il est en tout cas celui qui, le premier, a démontré avec un projet viable qu'il était efficace. En théorisant cela, Eric S. Raymond devient le fer de lance des hackers orientés vers le développement d'un écosystème du libre. Son coup de génie est de le marketer avec le concept d'open source, qui supprime l'ambiguité sur le terme free. En 1998, l'Open Source Initiative (OSI) est créée, chargée d'encadrer l'utilisation de ce nouveau terme.
Si l'open source a donné un sacré coup de pouce au logiciel libre, c'est un logiciel libre qui a mis de l'eau dans son vin, avec une multitude de licences approuvées dont certaines sont moins contraignantes. La licence BSD autorise ainsi que le code soit réutilisé dans un logiciel propriétaire. Mais au final, c'est toujours du code qui s'ouvre et le pré carré du logiciel propriétaire qui se réduit un peu. Et dès l'année du lancement de l'open source, le concept va bénéficier d'un sacré coup de publicité.

LA GUERRE DES NAVIGATEURS

Aujourd'hui, le libre a encore la réputation d'être une marotte pour geeks. Pourtant, votre maman utilise

sans doute sans le savoir un bel exemple de réussite : le navigateur Firefox représente 20% de part de marchés début 2012, et arrive en première position en Europe, même s'il est en perte de vitesse.
Firefox n'a pas toujours été un logiciel libre. Il est l'héritier de Netscape, le premier navigateur commercial grand public. Lancé en 1994, il devient vite hégémonique, faute d'une concurrence sérieuse. Par l'odeur des dollars du web alléché, Microsoft se réveille en 1995, avec ses manières habituelles, en mode rouleau-compresseur. Pour assurer le succès de son bébé Internet Explorer, la firme de Redmond l'installe d'office gratuitement sur Windows 95 et il est vrai aussi que ses progrès techniques lui assurent le succès auprès des utilisateurs. Netscape réplique en devenant aussi gratuit, en vain. Racheté par AOL en 1998, il se lance dans un bras de fer judiciaire en attaquant Microsoft pour ses pratiques déloyales.
Surtout, Netscape ouvre la même année son code source en le passant sous licence libre et créé l'association Mozilla.org pour le développer. À la plus grande joie d'Eric S. Raymond, qui écrit dans l'épilogue du *Bazar et la cathédrale*, intitulé *"Netscape embrasse la méthode du bazar !"* :
"Ça fait tout drôle de réaliser qu'on participe à l'Histoire... Le 22 janvier 1998, environ sept mois après ma première publication de cet article, Netscape Communications, Inc. a rendu public son projet de donner libre accès au code source de Netscape Communicator. Je n'avais pas la moindre idée que cela se produirait avant qu'ils ne l'annoncent.
Eric Hahn, vice-président et responsable en chef de la technologie à Netscape, m'a envoyé un courrier électronique peu après en me disant:
"Au nom de tout le monde à Netscape, je souhaite vous remercier pour nous avoir, le premier, aidés à comprendre tout cela. Votre réflexion et vos écrits ont été des inspirations cruciales dans la prise de cette décision. [...]
Netscape est sur le point de nous proposer une expérience à grande échelle, une expérience dans des conditions réelles du modèle du bazar dans une optique commerciale. La culture du logiciel dont le code source est ouvert affronte maintenant un danger ; si le projet de Netscape ne donne pas satisfaction, cela risque de jeter tant de discrédit sur le concept de logiciel dont le code source est ouvert qu'il faudra attendre dix ans de plus pour que des sociétés commerciales s'y intéressent."
La suite sera un peu plus complexe et moins commerciale que prévue mais ce choix finira par porter ses fruits et assure une belle visibilité à l'open source. Après une première version trop lourde, intégrant des fonctionnalités héritées de Netscape, le projet se recentre sur le développement du seul navigateur et aboutit en 2004 avec la première version de Mozilla Firefox. La fondation Mozilla, créée en 2003 pour assurer son développement, s'appuie sur la philosophie du libre :
"Nous sommes une organisation à but non lucratif qui se consacre à la promotion de l'ouverture, de l'innovation et des possiblités que peut offrir le Web. [...]
Nous pensons qu'Internet, en tant qu'élément majeur du développement social et technologique de notre temps, doit être amélioré et protégé.
La Fondation Mozilla est une organisation à but non lucratif qui se consacre à ces objectifs, mais la vraie force derrière Mozilla, ce sont les personnes du monde entier qui prennent part à la construction du Web qu'elles veulent."
Grâce à sa communauté de contributeurs qui améliorent Firefox et enrichissent ses extensions, l'hégémonique Explorer, endormi sur ses lauriers, est obligé de se réveiller : en dix ans, la balance a été renversée.
Pour clôre cette évocation de la part du libre dans le fonctionnement du web, il faut évoquer Apache.
Encore un nom qui ne vous dit rien, alors que ce logiciel de serveur web créé en 1995 est tout simplement devenu très vite majoritaire : sans lui, vous n'auriez pas accès à bon nombre de sites. Bon, certes c'est parfois une version propriétaire qui est utilisée mais la source est libre...

EXTENSION DU DOMAINE DU PIRATAGE

LES MARCHANDS...

L'évolution était prévisible : les terres vierges du Far West, arpentées depuis 20 ans par les audacieux défricheurs ont fini par attirer l'attention des prudents opportunistes. Avec le web, Internet touche désormais un grand public et cet espace a le potentiel d'un champ d'or. Il suffit que le législateur mette de jolies barrières et les années 1990 sont celles de la mise en place de ce cadre marchand.

Le même pays qui a donné naissance à l'Internet et au PC n'est pas le dernier dans la course aux enclosures. Les Etats-Unis marquent le coup avec le Telecommunications Act de 1996, qui dérégule le champ des télécoms. Le texte révise en profondeur un texte de... 1934 : sept ans après l'arrivé du web, l'Internet est enfin inclu dans le champ et cela donnera la bulle Internet, avec les dégats que l'on sait en 2000-2001. Le président Bill Clinton affirme alors que la loi *"stimulerait l'investissement, promouvrait la compétition et fournirait un accès ouvert pour tous les citoyens aux autoroutes de l'information."*

Ce qui n'est pas tout à fait faux : qui dit autoroute dit péage, bretelle d'entrée, bretelle de sortie. La même année, l'Organisation mondiale de la propriété intellectuelle (OMPI) émet ses recommandations dans deux traités qui, transposés par les différents pays, abaisseront d'un bon cran la barrière. C'est ainsi qu'en 1998, le Digital Millennium Copyright Act (DMCA) donne un coup de massue législatif. Il interdit en effet le contournement des mesure de protection numérique, les digital rights management (DRM), les "verrous numériques", la création, la distribution et l'utilisation d'outils et de services violant le droit d'auteur ou permettant de contourner les DRM. Au passage, ces dispositions conduisent à toucher à la neutralité du Net puisque le moteur de recherche Google est amené à retirer de son indexation des pages. Faites par exemple le test avec Pirate Bay :

> *En réponse à une plainte reçue dans le cadre du US Digital Millennium Copyright Act (loi de protection des droits d'auteur), nous avons retiré 2 résultat(s) de cette page. Si vous le souhaitez, vous pouvez prendre connaissance de la plainte DMCA qui a entraîné le retrait de ce(s) résultat(s) à l'adresse suivante : ChillingEffects.org.*
>
> Recherches associées à **Pirate Bay**

L'utilisateur sort grand perdant, comme l'analysait un juriste, en dépit de restrictions qui font figure de décoration pour la forme :

"On écarte donc en fait la plupart des restrictions qui, en vertu du copyright traditionnel, maintenaient un équilibre entre les intérêts des titulaires de droits et ceux du public en général, c'est-à-dire le citoyen ordinaire. Ainsi, non seulement la possibilité de fair use[48] *semble cruellement restreinte par le DMCA, mais cette loi vient également restreindre la diffusion de l'information d'une manière qui ne semble pas concorder avec l'esprit du Premier Amendement. Pourtant, rien ne permet de soutenir que les droits constitutionnellement garantis devraient perdre de leur sens ou de leur force dans l'environnement numérique."*

C'est pourtant ce rapport de force en faveur de l'industrie culturelle plutôt que la création et du public qui s'est imposé. Du moins dans les textes, car dans les usages, c'est un tout autre chemin qui est pris[49].

… ET LES PIRATES[50]

Sans eux, le business lucratif des majors de l'industrie culturelle aurait continué son train-train. Ses mécanismes basés sur une vision maximaliste du droit d'auteur n'auraient pas été contestés. Nous n'aurions pas accès de façon aussi facile à un immense catalogue de films et de musiques. Eux, ce sont Shawn Fanning et Sean Parker, deux (très) jeunes Américains, qui ont lancé en 1999 Napster, le premier site de partage peer-to-peer. Leur profil alimente la légende du jeune hacker génial qui révolutionne le

monde dans sa chambre : ces deux-là étaient faits pour se rencontrer. En ligne bien sûr.
À 16 ans, Sean Parker est arrêté par le FBI, son ordinateur saisi : le gamin est allé fouiner dans les réseaux de plusieurs multinationales et même des bases de données militaires. Poli, selon ses dires, il prévenait les administrateurs systèmes de ses intrusions, histoire que les brèches soient colmatées. S'il se fait chopper, la faute en revient à son père. Agacé de le voir passer des heures devant l'écran, il lui arrache son matériel des mains avant que l'adolescent ait le temps de se déconnecter.
Etudiant en informatique à la North West University de Boston, Shawn Fanning s'est mis en tête de développer un logiciel pour aider son colocataire à assouvir sa passion pour le rap : un logiciel qui facilite le partage de fichiers de musique en ligne au format mp3. Il met de côté ses études et code des semaines comme un fou. En janvier 1999 son logiciel est prêt. Il le baptise Napster, son pseudo qu'il utilise lorsqu'il va causer de hacking sur Internet, en référence à ses cheveux en bataille, "nappy" en anglais.
Quand Shawn et Sean se croisent sur IRC l'été de la même année, ça fait tilt et ils commencent à travailler ensemble au développement de Napster, avec l'aide de l'oncle de Shawn. L'outil est si révolutionnaire que son succès est phénoménal : il revendique un million d'utilisateurs en novembre, 20 millions d'utilisateurs en juillet 2000.
Mais devant le succès, le hobby devient vite une start-up attirant des investisseurs et la colère des majors et des artistes. Enfin une partie des artistes, car on assiste à une querelle des Anciens et des modernes : Metallica, Elton John, Paul Mac Cartney, Dr Dre s'en prennent aux "pilleurs" ; face à eux, The Smashing Pumpkins, Hole, The Offspring, Cypress Hill apportent leur soutien.
L'industrie musicale commet alors sa grande erreur en intentant un procès à Napster. Dès 1999, la Recording Industry Association of America (RIAA), son lobby américain, poursuit la compagnie pour violation du droit d'auteur, ainsi que ses soutiens financiers. Plutôt que de chercher à comprendre l'évolution de son business, l'industrie musicale opte pour la position défensive, s'accrochant à sa poule aux oeufs d'or que représentait le support physique de distribution. Si le site est fermé en 2001, avant de renaître sous une version légale, cette victoire n'est qu'apparente : elle a contribué à populariser le site dans le monde entier et a contrario son image en a pris un coup. Elle a stimulé l'élaboration de systèmes analogues encore plus perfectionnés, qui répondent à une demande nouvelle : les habitudes de consommation ont définitivement changé. Mais les offres légales satisfaisantes pour toutes les parties se font toujours attendre.

Berlin, novembre 2011, dans les locaux du Chaos Computer Club, influente organisation de hackers, fondée à Hamburg en 1981. Rencontre avec Andy Müller-Maguhn, longtemps porte-parole du CCC, qui revient sur la trajectoire de l'organisation et ses trente ans de hacking politique en Allemagne.

Berlin, novembre 2011. Les locaux du Parti Pirate. Le PP, en plein essor en Allemagne, a conquis 15 sièges au Parlement de Berlin. Plusieurs membres du CCC sont au PP. Andy Müller-Maguhn sur le Parti Pirate : *"C'est sympa le Parti Pirate. Nous verrons comment ils évoluent. Ce qui est intéressant, c'est de voir combien les autres politiciens ont peur de cette nouvelle organisation."*

L'ESSOR DE L'HACKTIVISME

L'EFF, LE GARDIEN DE LA FRONTIÈRE

Le 8 février 1996, en réaction au Telecommunications Act, John Perry Barlow écrit la très lyrique *Déclaration d'indépendance du cyberespace*, de Davos. Tout un symbole : le sommet annuel du Forum économique vient de se finir dans la petite ville suisse. Ce puissant texte définit l'Internet comme un lieu immatériel régi par des lois qui ne sont pas celles du monde des atomes, logique propriétaire contre éthique hacker, ancien contre nouveau monde :

"Vous n'avez pas pris part aux grands débats qui nous ont réunis, et vous n'avez pas non plus créé la richesse de nos marchés. Vous ne connaissez ni notre culture, ni notre éthique, ni les codes non-écrits qui ordonnent déjà notre société mieux que ne pourrait le faire n'importe lequel des règlements que vous prétendez nous imposer.

Le cyberspace est fait de transactions, de relations et de pensées, circulant en un flot ininterrompu sur nos canaux de communication. Notre monde est à la fois partout et nulle part, mais il ne se trouve pas là où vivent les corps.

Nous sommes en train de créer un monde ouvert à tous, sans privilège ni préjugé qui dépende de la race, du pouvoir économique, de la puissance militaire ou du rang à la naissance.

Nous sommes en train de créer un monde où chacun, où qu'il soit, peut exprimer ce qu'il croit, quel que soit le degré de singularité de ses croyances, sans devoir craindre d'être forcé de se taire ou de se conformer.

Les concepts de votre droit en matière de propriété, d'expression, d'identité, de mouvement et de circonstances ne s'appliquent pas à nous. Ils ont leur fondement dans la matière, et il n'y a pas de

matière ici.”
L’EFF ne se contente pas de clamer de grands principes éthérés, elle agit, avec son armée de juristes, en prenant part à la litanie de procès, qu’ils concernent la propriété intellectuelle, les DRM, ces verrous numériques, la liberté d’expression ou bien encore la défense de la vie privée. À l’actif de son lobbying, elle réussit à faire reconnaître en 1996 que le code d’un logiciel relève du Premier Amendement, celui qui consacre la liberté d’expression comme un droit fondamental, dans le cadre de l’affaire Bernstein contre le département de la Justice. Une affaire qui a pour centre un logiciel de chiffrement des communications, une des grandes batailles des années 90.
L’organisation franchit même la ligne blanche pour plaider cette cause avec le challenge du DES, le standard mis en place dans les années 70. Un algorithme tenu secret, au mépris du vieux principe de Kerckhoffs, qui postule que la sécurité d’un outil de chiffrement ne doit reposer que sur le secret de sa clé : cacher la recette empêche les gens de le tester et de l’améliorer.
En 1997, le directeur du FBI déclarent, vantards, que DES protège efficacement le secret des documents car il nécessiterait de complexes et coûteuses machines pour être cassé, et que cela prendrait du temps. L’EFF relève le défi et construit en 1998 le DES cracker, une machine peu chère - enfin tout est relatif, 250 000 dollars tout de même... - qui casse avec succès la clé du DES en 56 heures.
Parmi la fine équipe mise en place dans ce challenge, on trouve Philipp Zimmermann, un activiste écologiste qui a mis en ligne en 1991 le code source du logiciel d’encryptage qu’il vient de développer, Pretty Good Privacy (PGP, “plutôt bonne intimité”). Un projet de loi présente cette année l’a convaincu de l’utilité de violer la législation. *“Si cette résolution était devenue une véritable loi”*, expliquera-t-il dans son célèbre ”Pourquoi j’ai créé PGP”, *cela aurait contraint les fabricants d’équipements de communications sécurisées à insérer des ‘portes dérobées’ spéciales dans leurs produits, de telle sorte que le gouvernement puisse lire les messages cryptés par n’importe qui.”* L’enjeu est donc la défense des libertés fondamentales : *“utiliser PGP est bon pour préserver la démocratie.”* Et a contrario, c’est un outil vital pour les opposants des régimes autoritaires.
L’initiative n’est pas du goût du gouvernement américain, qui lui intente un procès en 1993, où l’EFF prête son concours. L’administration américaine apporte involontairement de l’eau à son moulin avec sa puce Clipper, un outil de cryptographie mis au point par la National Security Agency, dont l’algorithme est aussi secret. Elle concrétise les craintes soulevées par le projet de loi de 1991. L’EFF monte bien sûr au créneau avec ses confrères de l’Electronic Privacy Information Center (EPIC). Un an après, un chercheur publie le résultat de ses travaux qui confirme les craintes : Clipper présente une grosse faille de sécurité.
L’annonce préfigure la suite du procès : en 1996, les poursuites seront abandonnées et l’exportation des outils d’encryptage sera régularisée en 1999 aux Etats-Unis. En France, la libéralisation se fera en deux temps, 1996 puis 2004 avec la Loi pour la confiance en l’économie numérique (LCEN). C’est donc une demi-victoire puisque ce n’est pas le seul amour des libertés fondamentales qui a motivé le législateur mais celui du commerce en ligne, qui ne peut vraiment exploser que si les échanges sont bien sécurisés. Merci qui ? Merci les hackers qui cherchent les failles.

LES EXPLOITS DE FAILLE

Chercheur inlassable de failles, le Chaos Computer Club poursuit sa série des clacks d’anthologie. En 1996, il donne une leçon au géant haï Microsoft, en démontrant qu’ActiveX, un système permettant d’utiliser des programmes sans les installer, qui tourne automatiquement sur son navigateur Internet Explorer, n’est pas sécurisé. Il est possible de détourner de l’argent via Quicken, un programme de gestion des finances qui permet de faire des paiements électroniques. La leçon a lieu en direct à la télévision, avec un certain sens du spectacle. Un membre du CCC se connecte à un site affichant *“Comment devenir un millionnaire en cinq minutes”* et le code malicieux du CCC rajoute une transaction qui atterrit directement sur un compte créé pour la démonstration par le CCC.

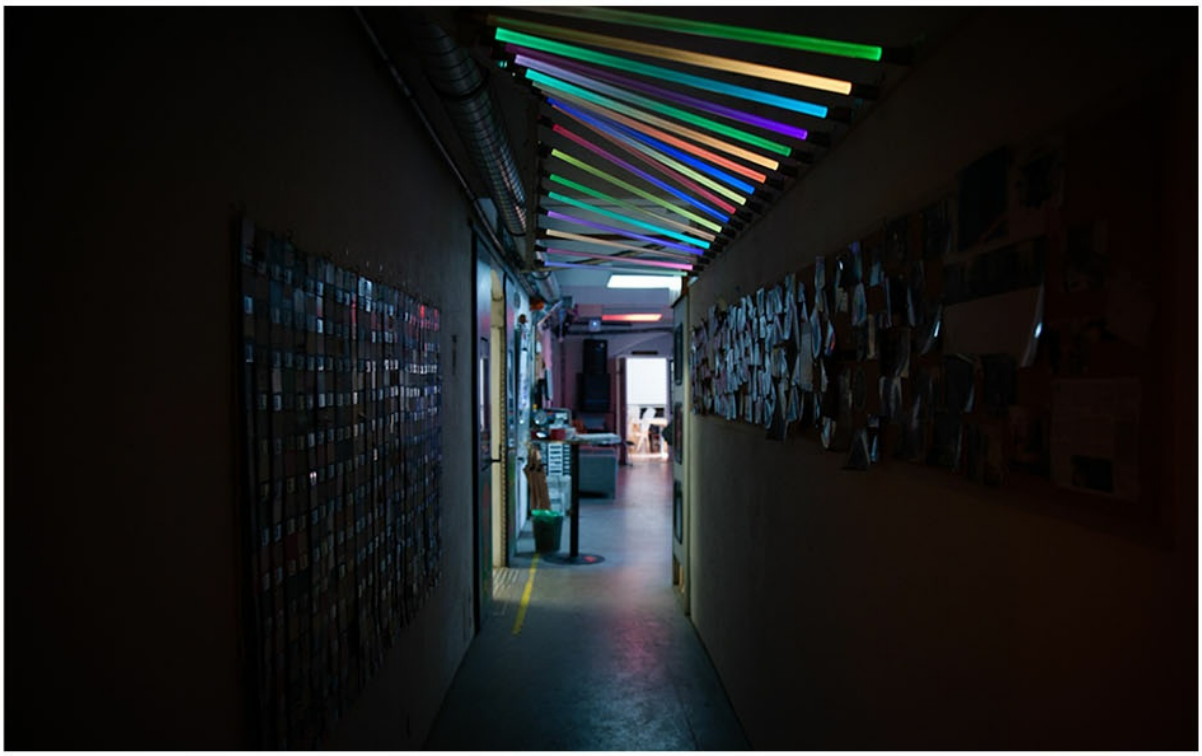
L'année d'après, ce sont les GSM qui font les frais de leurs recherches : ils ont réussi à dupliquer les cartes SIM des téléphones, ce qui permet tout simplement de passer des appels aux frais du propriétaire de la carte SIM.
Microsoft se prend aussi une belle volée avec Back orifice, le hack le plus célèbre de The cult of the Dead cow, présenté lors de DefCon 1998. Ce programme codé par Sir Dystic prend tout simplement à distance le contrôle des ordinateurs équipés du système d'exploitation Windows, qui domine le marché des OS. Si le programme peut faire l'objet d'un usage malveillant, il rend doublement service pour cDc : permettre d'administrer à distance et montrer que "le Leviathan" a "une approche emmental" de la sécurité de ses produits :
"Les deux buts légitimes principaux de BO sont de remplacer l'assistance technique et le contrôle des employés et d'administrer (un réseau Windows). On fera en sorte que Back Orifice soit disponible pour chaque personne qui prendra le temps de le télécharger. Alors, quelles sont les implications pour ceux qui ont adhéré / souscrit à l'approche emmental suisse de la sécurité par Microsoft ? Beaucoup, selon Mike Bloom, le directeur technique de Gomi Media à Toronto.
"L'apprentissage que j'observe autour de moi de nos jours c'est d'apprendre à se protéger, rentrer à la maison et regarder Jerry (Springer Show, ndlr). Microsoft a capitalisé là-dessus, au détriment de la valeur de la production, ce qui a eu un impact au niveau de la sécurité. Une opération comme le lancement (de Back Orifice) signifie que le plus petit dénominateur commun d'utilisateurs devra réussir à comprendre la menace, et que ce n'est pas Sir Dystic qui créera une application pour potentiellement mettre à mal la sécurité de Win32[51]. Microsoft s'est mis lui-même dans cette position où n'importe qui peut télécharger une application (ou créer la sienne), apprendre quelques astuces et provoquer de sérieux trucs / dégâts."
Succès immédiat et démenti attendu de Microsoft : *"Ce n'est pas un outil que nous devrions prendre au sérieux, ou que nos clients devraient prendre au sérieux"*, déclare Edmund Muth, en charge de la sécurité au sein de la direction marketing. Ce qui agace encore plus les hackers : la sécurité relève du marketing...

À L'ATTAQUE !

En parallèle de ces actions "classiques", des groupes s'hacktivent pour faire entendre leur voix politisée, dans la continuité de la cyberculture des années 70. Cette "electronic civil disobedience" (ECD) ne fait d'ailleurs pas l'unanimité dans le milieu des cyber-activistes. Ils utilisent un nouvelle arme, l'attaque par Distributed Denial of Service (DDoS) qui consiste à faire tomber un service en ligne en le saturant de requêtes, souvent un site Internet. Un mode de contestation dont le succès ne se démentira pas.
Les Zippies ("zen inspired pronoia professionals") auraient été les premiers à l'utiliser, dans le cadre de leur opération "Intervasion du Royaume-Uni". Par ce sit-in virtuel, ces activistes californiens protestent contre le Criminal Justice and Public Order Act, proposé par le gouvernement conservateur de John Major. Les Zippies sont particulièrement contris pas la mesure qui réprime les raves en extérieur. Leur opération est lancée un 5 mai, jour de la fête célébrant Guy Fawkes, une figure historique symbolisant l'opposition au pouvoir central, et qui connaîtra dix ans plus tard une célébrité mondiale avec le film *V pour Vendetta* et les Anonymous[52]. Un des participants se souvient :
"C'était la première fois qu'on utilisait cette tactique en ligne pour les besoins d'une désobéissance civile légitime, ce qui nous a précipité dans ce nouvel âge de la 'guerre de l'information et de la cyberguerre'.
'Ça aura le même impact sur Internet que la place Tian'anmen en a eu sur les fax' pouvait-on lire sur l'un des flyers d'Intervasion distribués par email. 'Tim Leary vous veut pour l'Invasion Virtuelle de la Grande-Bretagne' déclarait un autre, alors que la protestation accompagnait le lancement du livre de Leary, Chaos et Cyberculture, *où les Zippies intervenaient pour 'kidnapper Tim et le forcer à pirater la page web de John Major', selon son éditeur Ronin Press."*

En 1999, les Electrohippies joignent leurs voix à ceux des altermondialistes qui manifestent lors du sommet de l'Organisation mondiale du commerce (OMC) à Seattle en 1999. Au blocage du sommet par les opposants dans les rues, les electrohippies ajoutent celui des sites, avec plus ou moins de succès. Les e-hippies expriment leur credo dans un manifeste, anti-gros capital mais pas anarchiste pour autant :
"Nous ne sommes pas contre le gouvernement, mais nous sommes pour le gouvernement qui représente les besoins du peuple, qui travaille pour pourvoir à ces besoins et services dans leur intérêt, et dont les actions quotidiennes ne sont pas soumises à des influences extérieures pour répondre aux besoins d'une minorité dans une société envahie par les entreprises."
Mixant artivisme et hacktivisme, Ricardo Dominguez lance le collectif Electronic Disturbance Theater en 1997. L'EDT prend pour cible le gouvernement mexicain, qui réprime l'Armée zapatiste de libération nationale, un mouvement anti-impéraliste autonomiste porté par les Indiens du Chiapas. L'EDT crée un outil qui facilite les attaques DDoS, FloodNet, une idée là encore reprise plus tard.
Issu de la tendance hackers hardcore, Legions of the Underground (LoU) déclare la *cyberguerre* à l'Irak et la Chine en 1999, où du moins certains hackers se revendiquant de LoU. LoU est contraint de faire une publication officielle dans *2600* pour clarifier la situation qui soulève plusieurs questions encore d'actualité avec les Anonymous : quand on est un groupe peu structuré, comment conserver une cohérence dans son discours et ses actes ? Qu'est-il juste de faire au nom de la défense de la liberté d'expression et d'information ?
"Avec la taille de LoU, qui compte plus de 20 membres, et notre organisation informelle, nous réalisons qu'il peut être difficile de vérifier que quelqu'un est bien membre. Ce qui a probablement conduit à cette vague d'imposteurs LoU, qui ont fait de fausses déclarations à notre propos et sur nos actions. En bref, au nom des membres de LoU, j'aimerais déclarer que nous n'avons entrepris aucune action qui aurait pu endommager les réseaux ou systèmes chinois ou iraquiens, ni même n'importe quel autre système ou réseau du monde, et nous n'avons pas l'intention de le faire. En outre, le LoU ne s'est allié, affilié ou ne travaille avec aucun autre groupe quel qu'il soit. Au sein de LoU, nous tenons à notre intégrité et nous avons un sens profond de l'éthique. Nous ne souhaitons rien de plus qu'un traitement juste et équitable pour tout le monde, et nous ne voulons rien d'autre qu'un éclairage positif sur la communauté hacker."
Plusieurs prestigieux collectifs de hackers se joignent aussi à eux dans un communiqué commun. Cette éthique et surtout cette politisation est fermement réaffirmée la même année par un nouveau groupe, issu de The cult of the dead cow, fondé par Oxblood Ruffin. Hacktivismo invite solennellement la communauté des hackers à agir dans sa déclaration :
"Nous sommes TRÈS SERIEUSEMENT INQUIETS de l'extension de la censure de l'internet par les gouvernements, soutenus par les sociétés transnationales, PRENANT POUR BASES les principes et objectifs inscrits dans l'Article 19 de la Déclaration Universelle des Droits de l'Homme (UDHR) qui déclare que "Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit", ainsi que l'Article 19 du Pacte international relatif aux droits civils et politiques (ICCPR) [...] NOUS SOMMES DE CE FAIT CONVAINCUS que la communauté internationale des hackers se doit dorénavant de réagir."
Plus de dix ans après, son credo est malheureusement encore d'actualité, décliné par de multiples autres groupes d'hacktivistes. Encore bien occupées par la lutte pour les libertés numériques, les années 2000 voient aussi naître de nouvelles espérances, ancrées dans le monde bien tangible des atomes.

HELLO HACKERSPACES Esther Schneeweisz, alias Astera, et son bras tatoué, à Berlin en novembre 2001. Astera, commence son parcours de hackeuse au Metalab de Vienne en Autriche. Elle est la co-fondatrice d'hackerspaces.org le site qui liste les hackerspaces du monde entier. Les hackerspaces se développent hors d'Europe à partir d'une conférence donnée en 2007 au Chaos Communication Camp.



Le Metalab, hackerspace fondé en 2006 en Autriche est situé au coeur de Vienne, entouré des palais de l'ex-empire austro-hongrois. Outre ses réserves de Club Mate, les 200m² du Metalab acceuillent un laboratoire de chimie et de photo, une découpe-laser, des imprimantes 3D et des salles de réunions. Plusieurs start-ups y ont vu le jour dont Soup.io, le tumblr des hackers, fondé par C3o, ou les premiers prototypes de la MakerBot.

Le HSBP, (HackerSpace BudaPest) et ses nouveaux locaux trouvés en urgence, dans un petit sous-sol du centre ville. À la manière du hackerspace de Madrid (le Hamlab), le hackerspace de Budapest était situé dans une sorte de squat qui fait toujours office de à bar, centre culturel et associatif, jardin, scène de théâtre...

IV. HACKERS ON PLANET EARTH[53]

Dès lors que le hack est un état d'esprit, il s'applique à tout, y compris à nos objets du quotidien. Dans les années 2000 une autre révolution se dessine, celle de la fabrication numérique personnelle, rendue possible par la baisse du coût du matériel, l'amélioration des logiciels et la puissance collaborative d'Internet. Désormais, il est possible pour un prix relativement abordable d'avoir une mini-usine dans son garage. *"En bref, les atomes sont les nouveaux bits"*, résume Chris Anderson, le rédacteur en chef de *Wired*. Et comme les hackers ont contribué à la première, ils mettent la main à la patte. De puce électronique, s'entend : c'est le triomphe du Do-It-Yourself, ("fais-le toi-même", DIY en abrégé), version moderne et sexy du bricolage de grand-papa.

"LA PROCHAINE RÉVOLUTION ? FAITES-LA VOUS-MÊME" [54]

HACKERS ET MAKERS

Avant de découvrir plus avant cette nouvelle révolution, arrêtons-nous un instant sur la terminologie. Autour du petit monde des hackers gravite une autre planète, celle des makers. "Maker" désigne une personne qui bidouille les objets physiques. On aurait tort de s'arrêter aux étiquettes en les écartant du sujet : ils font partie d'une même galaxie. Ce serait vain aussi, tant ces mondes sont poreux car ils ont en commun d'encourager la réappropriation des techniques et le partage des connaissances et de porter cette révolution de la fabrication numérique personnalisée. Avec toutefois quelques nuances.

La puissante et très marketée communauté des makers ("créateurs") s'est constituée (en tant que concept) dans les années 2000 aux Etats-Unis, en particulier autour de Dale Dougherty, co-fondateur de l'éditeur de manuels de programmation O'Reilly media et tête de proue de MAKE. MAKE édite un magazine, lancé en 2005, organise des événements, les Maker Faire, qui rassemblent des centaines de milliers de personnes de par le monde, et propose un site de vente.

Contrairement à l'éthique hacker originelle élitiste, Dale Dougherty défend l'idée que *"nous sommes tous des créateurs"*, et reprend le mythe cher aux Américains d'un peuple qui s'est fait lui-même et a bâti son économie à la force de sa imagination. Lors de sa présentation à TEDx, il a montré une vieille publicité de Chevrolet intitulé "American maker" affirmant que *"parmi toutes les choses qui font de nous des Américains, il y a le fait d'être des créateurs."* Et il choisit pour illustrer cette figure des "*hobbyistes qui jouent à découvrir ce que la technologie peut faire"* pour le plus grand bien de l'économie notre fameux Homebrew Computer Club : *"les makers sont une source d'innovation et je pense que cela renvoie à quelque chose tel que l'apparition de l'industrie des ordinateurs personnels. [...] Des tas d'industries sont nées de cette idée de jouer et de comprendre les choses grâce à des groupes de travail."* La dimension éducative est donc aussi très importante.

Cette fibre patriotique a récemment conduit MAKE à accepter une bourse de la Darpa, l'agence de la recherche du Pentagone, dans le cadre d'un programme éducatif de la Darpa baptisé Mentor (Manufacturing Experimentation and Outreach), qui s'inscrit dans le projet Adaptive Vehicle Make, dont le but est de *"révolutionner la façon dont les systèmes de défense et les véhicules sont conçus."*

La décision a fait l'objet d'une vive polémique dans le milieu après que Mitch Altman a annoncé qu'il ne participerait pas à Maker Faire pour manifester son désaccord éthique. Voilà le vieux débat du temps de la guerre du Vietnam ravivé. Dale Dougherty justifie :

"Notre programme encourag[e] les écoles à impliquer davantage les enfants dans le "faire", en créant des makerspaces et en fournissant un accès à ces outils pour les projets d'étudiants, et à utiliser Maker Faire pour diffuser plus de travaux d'étudiants. Nous avons été motivés pour postuler à la bourse de la Darpa par la déclaration suivante qui faisait partie du programme Mentor : "un des

plus grands défis auquel nous faisons face en tant que nation est le déclin de notre capacité à fabriquer des choses". Dr Regina Dugan, alors directrice de la Darpa."
Face à une ligne de séparation qui tend à s'effacer, le débat a montré que le clivage pouvait ressurgir, comme l'explique Mathilde Berchon, qui a passé plusieurs mois dans la communauté des makers de San Francisco [55]:
"Le débat montre le clivage entre les vrais hackers, plus politisés, militants, certains sont même anarchistes, et l'essentiel des troupes, qui se reconnaît davantage dans la communauté maker. Le type-même, c'est le bon père de famille qui bricole dans son garage en buvant de la bière, qui aime son pays et veut le défendre, sans être un gros lourd patriote. Avec cette bourse, MAKE prend le risque de se couper de la frange la plus radicale."
Les makers et les hackers sont donc grosso modo sur une même ligne, qu'ils tracent avec des outils libres bien sûr.

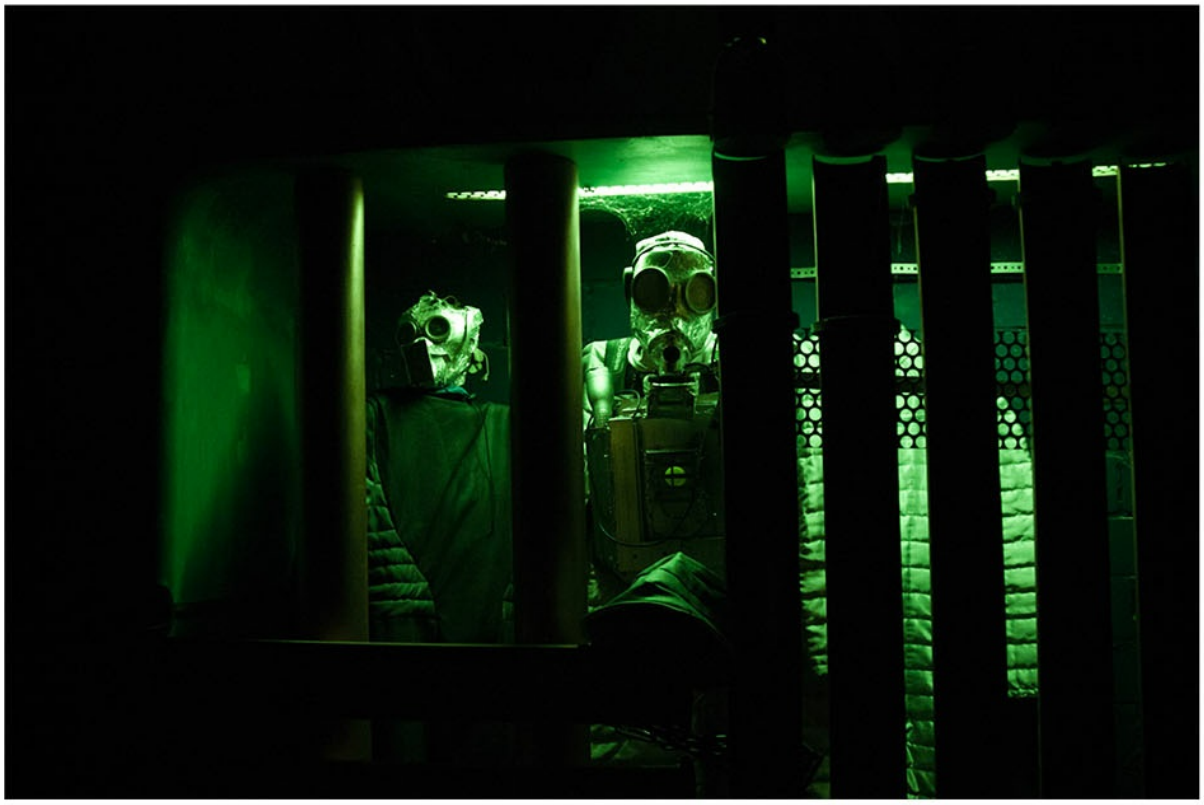
L'OPEN HARDWARE

Le matériel, le "hardware", suit la même bonne voie libre que le logiciel. Plus que du simple matériel, c'est donc toute une philosophie que l'open hardware promeut, comme l'explique Hackable Devices, une petite start-up pionnière de l'open hardware en France : [56]
"Le projet hackable-devices est né de la volonté de hackers de mettre à la disposition des autres hackers le matériel qui leur correspond. Beaucoup plus qu'une simple boutique en ligne, hackable-devices est une plateforme technique d'échanges autour du matériel et des appareils dont vous pouvez prendre le contrôle, que vous pouvez adapter, modifier, bidouiller ou améliorer. Les logiciels libres n'ont pas amené la liberté qu'au logiciel. Chez hackable-devices nous croyons sincèrement que le matériel et l'électronique peuvent être utilisés et développés selon les mêmes processus communautaires. Nous pensons que la culture du DIY et l'apprentissage par la pratique doivent être encouragés. Nous savons que les gens se rencontrent pour créer, améliorer et s'amuser tout à la fois. Nous sommes persuadés que les objets doivent réellement vous appartenir."
Concrètement, quand vous concevez un produit en open source, vous fournissez les plans du design, du circuit imprimés, des composants, etc, pour faciliter la reproduction de l'objet[57]. La réflexion sur les aspects juridiques a commencé en 2010 lors du premier Open Hardware Summit, avec un cadre initial posé. Depuis, des licences spécifiques ont été élaborées, comme la TAPR, celle du CERN, la Hardware Design Public License, etc.
L'open hardware a déjà ses produits, ses entreprises et ses apôtres. L'imprimante 3D est la petite reine incontournable, qui se démocratise comme naguère le PC. Une imprimante 3D, c'est tout simplement un outil qui imprime, couche après couche, l'objet que vous avez dessiné avec un logiciel de conception assistée par ordinateur (CAO). Cela sert aussi bien à remplacer un objet cassé ou perdu qu'à créer ceux dont vous avez besoin. Le modèle RepRap, auto-réplicant, a été créé par Adrian Bowyer, un ingénieur et mathématicien aux envolées révolutionnaires :
"Plus personne ne fait appel à une société d'impression pour faire des cartons d'invitation pour une fête, ils utilisent leur imprimante. Maintenant imaginez un monde ou presque tous ces produits conçus par des ingénieurs sont comme ces cartons d'invitation… "
La MakerBot, développée par Bre Pettis, Adam Mayer et Zach Smith du hackerspace américain NYC Resistor, est un carton dans le milieu. Comme ce sont des machines open source, elles sont améliorées par les utilisateurs : alliant les avantages des deux, l'Ultimaker des Hollandais du fab lab Protospace (voir ci-dessous) est plus puissante et efficace. Comme les pionniers du PC n'avaient d'autre choix que de se retrousser les manches, ces imprimantes 3D sont vendues en kit et les monter est en soi un petit challenge. Sur un site comme Thingiverse, les gens partagent les plans de leurs objets pour en faire bénéficier tout le monde. Même The Pirate Bay a ouvert une section dédiée. L'impression 3D ouvre des possibles pour tous, comme l'ordinateur naguère... à condition que la logique propriétaire du vieux

monde ne foute pas tout en l'air.
Arduino est un autre incontournable de la panoplie. Comme MINIX a été développé dans un but éducatif, ce microprocesseur a été conçu par l'Italien Massimo Banzi pour apprendre aux étudiants à développer des projets en électronique. Peu cher, le prix *"d'un repas dans une pizzeria"*.
Pour s'initier, le site de vente en ligne Adafruit est un site incontournable, avec ses kits et ses tutoriels vidéos. Créé en 2005 par Limor "Ladyada" Fried, une ingénieur du MIT pionnière de l'open hardware, Adafruit est une petite entreprise florissante.
La liste des réalisations est longue en open source : tout, tout, vous ferez tout, en fonction de vos capacités bien sûr. Entre de la bière ou un support mural de rasoir et une voiture ou même une maison entière, il faut quelques heures d'entrainement et un solide crowdsourcing, ce recours à l'intelligence collective facilité par Internet.
L'open hardware encourage les velléités chez bien des bricoleurs du dimanche, trop du dimanche peut-être, et des voix s'élèvent du coup chez les hackers/makers les plus pointus pour critiquer la basse qualité des objets créés. Au moins s'occupent-ils pacifiquement dans leur garage...
Et si l'open hardware permet aux gens de se réapproprier les technologies et de libérer leur créativité, il a aussi engendré un véritable écosystème. Et l'enjeu sera ausi de maintenir les valeurs : et voilà que le vieux débat de la fin des années 70 ressurgit aussi. La dimension éthique se pose également pour les composants, qui ont une fâcheuse tendance à venir de Chine[58].

Nanterre, hiver 2011. Les membres du jeune hackerspace Electrolab se préparent une tambouille après la réunion hebdomadaire de leur association. Il en faut de l'énergie pour installer les machines et achever les travaux. L'Electrolab est dédié à l'électronique, la chimie.

"Be future compatible" : le hackerspace de C-BASE à Berlin est une station spatiale… du futur. Vieille de 4 milliards d'années, elle se serait crashée à Berlin en 1995… On y entre comme dans un vaisseau du film Star Wars, on en sort les yeux plein d'étoiles et de néons. L'immense C-BASE, forte de 300 membres accueille aussi les communautés WiFi, les wikipédiens berlinois, des conférences du CCC, des concerts…



“CE RÉSEAU DE HACKERSPACES VA CHANGER LE MONDE COMME JAMAIS”

Depuis 1999, le Chaos Computer Club organise un grand camp quadriannuel qui rassemble des hackers du monde entier. Une bouteille de Club-Maté à la main, la boisson préférée des hackers boostée à la caféine, les participants du Chaos Communication Camp participent à de multiples ateliers, écoutent des conférences, ou tout simplement discutent avec leurs voisins de tente.

L’édition de 2007 est marquée par une conférence[59] qui aura un impact sur la communauté mondiale : l’expansion des hackerspaces, ces espaces physiques où les hackers se rencontrent. Parmi l’assistance, on trouve Mitch Altman, fervent partisan de l’open hardware et roi du fer à souder. Aujourd’hui encore, il en garde un souvenir ébloui, et pour cause :

“Il a changé ma vie à jamais et celle de tant de gens. Je ne suis pas venu ici en pensant que ça marquerait le début d’un mouvement mondial mais ça a été le cas. Trois hackers allemands ont juste fait une conférence expliquant comment lancer des hackerspaces. Comme nous avons prospéré, d’autres s’y sont mis et ont prospéré, et maintenant ils sont maintenant plus de 900 listés sur hackerspaces.org, tout autour du monde. Ce réseau déjà existant va changer le monde comme jamais.”

Lors de leur exposé, nos hackers ont présenté le Hacker Space design Pattern, un document que *“tout hackerspace enthousiaste devrait étudier au moins une fois dans sa vie.”* Enrichi depuis, c’est un précieux guide pour monter et faire tourner son hackerspace, dont la structure reproduit celle de Design Patterns, consacré lui aux logiciels.

Outre Mitch Altman, donc, on croise aussi une poignée d’Américains qui voyagent dans un antique avion de la compagnie Hackers on the Plane. Cette sorte de Tour Operator pour hackers a été montée par Nick Farr, qui a aussi lancé la Hacker Foundation pour financer les hackers qui font de la recherche. De retour aux Etats-Unis, ils mettent en application ces bons conseils, à commencer par Mitch Altman qui fonde la même année NoiseBridge à San Francisco avec son ami Jacob Applebaum, un des principaux architectes du système de navigation anonyme Tor, utilisé par tous les dissidents du monde[60].

Ce qui exalte notre pape du fer à souder et bien d’autres, c’est que les hackerspaces permettent à leurs membres de se rencontrer, d’échanger, de faire avancer leurs projets ; on s’entraide, on mutualise le matériel, on fait des commandes groupées. Ils sont en quelque sorte l’avatar moderne du Home Brew Computer Club, à ceci près que le champ du hacking s’est étendu au monde solide. La multiplication des hackerspaces est aussi la suite logique de l’Histoire :

“L’idée de hackerspace [...] définit fortement le mouvement global des hackers au 21e siècle. Tandis qu’Internet a ouvert la communication intercontinentale, il a en fait fait valoir des espaces de réunions réels, physiques, où vous pouvez mettre un visage sur un e-mail. Alors que le village global a été la vision dès le début, c’est dans les hackerspaces que ce rêve devient réalité.”

Lieux ouverts, pour peu qu’on n’y viennent pas avec des gros sabots de journalistes en quête de cybercriminel, les hackerspaces contribuent à ce que la cité s’ouvre aux hackers :

“Les geeks et les nerds sont souvent représentés assis seuls derrière la lueur d’un écran de portable mais maintenant, dans de nombreuses villes grandes et petites du monde entier, des hackers se rassemblent pour souder de l’électronique, partager des compétences en programmation, enseigner à des classes et construire une communauté de gens intelligents et curieux.”

Le *Guardian* va même jusqu’à faire la comparaison, lourde de promesses, avec les *“cafés anglais du siècle des Lumières. Ce sont des lieux ouverts à tous, sans distinction de statut social, où priment les idées et les connaissances. Dans l’Angleterre du XVIIème siècle, l’égalité sociale et la méritocratie qui régnaient dans les cafés étaient tellement troublantes pour le pouvoir que le roi Charles II avait tenté d’interdire ces lieux. C’est dans les cafés que les informations jusqu’alors détenues par les élites, étaient partagées avec une classe moyenne qui commençait à émerger. On leur doit bien des*

réformes sociales qui ont transformé la vie publique anglaise."
Et aujourd'hui, les hackers vont même sur les routes au volant de leur hackbus à la rencontre des gens, répandre la bonne parole.
Chaque hackerspace a sa spécificité, en fonction de son histoire et des membres qui la compose. Les Italiens de Verde Binario ("binaire vert") sont ainsi spécialisés dans le recyclage des ordinateurs, les Français de l'Electrolab travaillent sur des modes de déplacement électriques, vélo, trotinette, voitures, etc., les Allemands du CCC de Berlin sont toujours très en pointe sur la sécurité et la privacy, BioCurious est dédié au biotechnologies, etc.

DE L'OCCIDENT AUX PAYS ÉMERGENTS

Dans les pays en voie de développement, les hackerspaces trouvent un terrain de développement particulièrement favorables car beaucoup de personnes sont des hackers qui s'ignorent : ils bidouillent parce qu'ils n'ont pas le choix, par contrainte financière. Ils ont donc tout intérêt à se retrouver dans ce type de lieu communautaire qui favorise l'entraide. Tarek Ahmed, le fondateur du jeune Cairo Hacker Space résume :
"Nous avons plus que tout autre chose besoin de hackerspaces car c'est parfait pour des pays qui ont des problèmes économiques."
Les hackerspaces servent du coup à dynamiser le tissu des entreprises en aidant l'éclosion de start-ups dans les nouvelles technologies, aux frontières parfois de l'incubateur de projets ou de l'espace de co-working. On y pratique du coup peut-être un hack plus pragmatique, comme l'explique Bosun Tijani, fondateur du Nigeria HUB – Co-creation Hub, dans une pichenette indirecte aux hackers "embourgeoisés" des pays occidentaux :
"Nous avons beaucoup de hackers ici qui réinventent la roue, notre façon de les encourager consiste à les amener à se centrer sur des problèmes réels et la meilleure façon, c'est de les mettre avec des gens qui comprennent les problèmes réels, c'est notre raison d'être. L'intérêt pour les hackerspaces croîtra en continuant de démontrer le bien qu'ils peuvent apporter à l'Afrique. Nous devons cultiver la culture de l'utilisation des connaissances dans le cadre de problèmes locaux et les hackerspaces encouragent l'application des connaissances et de nouvelles façons de résoudre des problèmes."
Jusqu'à présent fournisseuse des hackerspaces du monde entier en matériel, bas prix oblige, la Chine a commencé aussi à ouvrir des espaces en 2010, à l'initiative d'expatriés qui ont pu se frotter au concept. Le tropisme économique est aussi bien présent. Ricky Ng-Adam, un Canadien qui a co-créé le premier hackerspace chinois à Shanghai en convient :
"La Chine est un endroit très propice, d'abord, parce que la technologie joue un rôle primordial au développement économique et avec beaucoup moins de controverse. Ensuite, dans un pays où le guanxi (relations interpersonnelles) jouent un rôle primordial, il est parfois difficile pour les Chinois qui sont à l'extérieur des organisations reconnues et légales, assez limitées, de créer ce genre de connexion. Un hackerspace permet aux plus jeunes de se rencontrer et de bâtir un réseau qui leur est propre à travers des projets collaboratifs plutôt que des repas bien arrosés et enfumés. Certains participants chinois font effectivement pression pour transformer l'espace en incubateur ou espace purement commercial et ont de la difficulté à percevoir les avantages non-monétaires de participer dans un tel espace. Souvent, la question clé de leur part concerne nos "profits."
Il a d'ailleurs lui-même démarré une entreprise avec un partenaire rencontré dans son hackerspace, un ingénieur électronique chinois. Leur idée ? Viser les hackers avec un produit de niche, un super Arduino. De même, Eric Pan, un des organisateurs de Maker Faire Shenzen, a créé Seeed Technology, une société spécialisée dans le hardware open source, et co-fondé Chaihuo makerspace.
Le potentiel est si fort que même l'Etat chinois encourage leur développement, comme en témoigne le projet ToyHouse, qui vise les écoles, ou bien encore les fonds que la province de Shanghai veut apporter aux hackerspaces. Une façon aussi de surveiller ce milieu qui par définition rejette tout régime

restreignant la circulation de l'information, un sport où la Chine excelle. Le futur dira qui récupèrera qui...

LES FABULEUX FAB LABS

Aussi utiles dans les pays émergents mais dédiés exclusivement à la fabrication numérique, les fabrication laboratories, les fab labs attirent naturellement les hackers qui se retrouvent dans le concept. Ce mouvement est parti des Etats-Unis, plus précisément d'un endroit que l'on a déjà croisé sur notre route, au tout début : le MIT. Au début des années 2000, le physicien Neil Gershenfeld met en place un cours de prototypage rapide intitulé "How to make (almost) anything" (Comment fabriquer (presque) n'importe quoi). Initialement destiné à aider les élèves à finir leur projet d'études, il met à leur disposition un lieu avec des machines assistées par ordinateur et tout l'outillage nécessaire. Mais l'endroit est vite utilisé pour satisfaire leurs envies, hors des heures de cours. Cela vous rappelle quelque chose ?

Neil Gershenfeld rajoute un vernis de marketing en structurant le concept sous le nom de fab lab, encadré par une charte, et s'appuyant sur un réseau désormais mondial reconnaissable à son logo. Au centre de ses valeurs, le partage des connaissances et l'éducation : les utilisateurs doivent apprendre à faire eux-mêmes, avec l'appui des autres membres.

Cet artisanat high-tech essaime sur tous les continents, aussi bien au Ghana qu'en Norvège ou Indonésie. Le potentiel est infini puisqu'il met à disposition des moyens jusque-là réservés à l'industrie traditionnelle. Il permet de satisfaire des micro-marchés qui ne semble pas intéressant économiquement à cette dernière ou un "mono-marché" lorsque l'utilisateur vient y concevoir un produit dont il aura seul l'usage. Il apporte aussi une réponse au problème de ce que certains ont théorisé sous le concept d'obsolescence programmée : nos objets de consommation courante sont conçus pour avoir une durée de vie limitée. Le fab lab facilite la réparation en permettant par exemple de faire une pièce sur mesure pour remplacer celle qui a cassé dans votre appareil électro-ménager. Très clairement, le discours de Neil Gershenfeld trouve un écho dans le discours décroissant qui entend hacker la société de consommation actuelle : *"Il s'agit de créer plutôt que de consommer."*

Toutefois, sa charte assez souple sur l'aspect business en fait aussi un lieu intéressant pour une start-up qui souhaite faire une preuve de concept. Et tant que la charte est respectée, une entreprise tout ce qu'il y a de plus classique peut ouvrir un fab lab, ce qui permet de se donner une image de société innovante et sympathique à moindre frais. Sans compter celles qui s'approprient le nom sans respecter la charte...

L'HACKTIVISTE EN OUVERTURE DES JT

Contrôler, encore et toujours plus

Dans les années 2000, les législations visant à renforcer la protection de la propriété intellectuelle et du droit d'auteur se multiplient dans le monde entier. Le lobby de l'industrie culturelle, arquebouté sur la défense de ses intérêts, souffle avec efficacité à l'oreille des parlementaires. Après le DMCA américain, l'Europe emboîte le pas avec deux textes qui donnent le la répressif dans l'Union européenne : les directives EUCD (European copyright directive) et IPRED (Directive on the enforcement of intellectual property rights) de 2001 et 2004. Aux Etats-Unis, les lois Stop Online Piracy Act (Sopa, 2011) et Protect IP Act (Pipa, 2011) suscitent la bronca de par le monde. Tout comme l'accord commercial anti-contrefaçon (Acta), poussé par plusieurs pays dans la discrétion avant d'être révélé au grand jour. Autant de noms absconds mais qui ont des conséquences bien tangibles sur les internautes. Qui n'a pas dans son entourage une personne qui a reçu une lettre de la Hadopi ? Et peut-être même vous en personne, cher lecteur :) Et bien cette fameuse loi anti-piratage est issue indirectement de l'EUCD.

Le jeu du chat et de la souris se poursuit, c'est à qui maintiendra un pas d'avance. D'un côté, les techniques de partage de fichiers sont perfectionnées et s'adaptent sans cesse face à l'évolution de la législation, dans une belle illustration de la résilience de l'Internet. L'ancêtre Napster a ainsi été remplacé par des outils décentralisés comme Emule ou Limewire, puis les annuaires de liens et la technique BitTorrent, plus rapide, ont pris le relai. Le peer-to-peer a cédé, de force juridique, du terrain, remplacé par le streaming (écoute à la demande) et le direct download (téléchargement direct), avant de faire son retour, mais mieux protégé contre le traçage grâce à des outils d'anonymisation.
La partie adverse module aussi son argumentaire et enchaînent les procès. En 2000, la Motion Pictures Association of America (MPAA), le lobby des gros studios d'Hollywood, parvient à faire condamner l'ezine underground *2600*. Il est jugé coupable d'avoir expliqué à ses lecteurs comment fonctionne DeCSS, un logiciel de visualisation de DVD qui casse des DRM empêchant de copier des DVD. *2600* n'a désormais plus le droit de publier le code source du logiciel incriminé ni de lien vers lui. En 2005, Sharman Networks, la société éditrice du logiciel de téléchargement peer-to-peer KaZaA est condamnée par la justice autralienne à verser 115 millions de dollars à l'industrie musicale, et doit équiper son logiciel d'un filtre anti-contrefaçon. En 2010, Limewire est contraint d'être retiré sur décision de justice et paye 105 millions de dollars aux labels de musique. Dans cette course à la judiciarisation, les utilisateurs sont aussi poursuivis, non sans dommages collatéraux.
Ce bref contexte serait incomplet si l'on omettait de préciser que le noble idéal du partage de la culture est parasité par des profiteurs qui y voit surtout une opportunité de monter une économie parallèle dont la lucrativité n'a rien à envier à celle des lobbys. À ce titre, le site de direct download MegaUpload, fermé en 2012 suite à une procédure juridique, et son fondateur Kim Dotcom, sa Porsche, sa villa de luxe et son majordome desservent surtout la cause du libre partage.
Ce combat s'inscrit dans le théâtre plus vaste et parfois plus dramatique de la lutte pour les libertés numériques. "*The information wants to be free*", plus que jamais, et les velléités de contrôle se renforcent. La neutralité des technologies font le lit des marchands d'armes numériques qui refourguent leur matériel à des dictateurs comme Kadhafi : ne s'agissait-il pas de lutter contre le terrorisme ?
En face, la mobilisation reste intacte, à l'image de la spectaculaire journée de blackout sur l'Internet américain, où l'on voit Google mettre ses pas dans ceux de Wikipedia, l'encyclopédie en ligne qui incarne cette vision d'une information ouverte et collective. Poil à gratter protéiforme, les hacktivistes multiplient les actions, en ligne et dans la rue. Héritiers de 30 ans d'hacktivisme, ils sont les chiens de garde d'une révolution que leurs prédécesseurs ont provoqué dans les années 70. À défaut d'évoquer toutes leurs foisonnantes manifestations, voici un florilège.

HACKER L'INTERNET

Fut un temps que les moins de 20 ans ne peuvent pas connaître où les connections WiFi étaient ouvertes, ce qui permettait de profiter gratuitement de la connexion du voisin. Aujourd'hui, en France par exemple, la loi Hadopi contraint les utilisateurs à "protéger" leur connexion s'ils ne veulent pas être accusés d'avoir facilité le téléchargement illégal à un utilisateur extérieur. Les mots de passe sont de rigueur, et peu importe que ce soit des parades-passoires.
Et il est encore des régions où l'accès à Internet passe par la mise en place de réseau WiFi. Comme ce sont des zones pas très peuplées, elles n'intéressent guère les gros opérateurs qui ne veulent pas les équiper sans être assurés d'un retour sur investissement.
Face à cette vision commerciale, des bidouilleurs se sont regroupés en communauté au début des années 2000 et ont choisi de collaborer ensemble pour développer des réseaux WiFi alternatifs : Freifunk en Allemagne, FunkFeuer en Autriche ou Guifi.net en Espagne, etc. Au coeur de leur démarche, les valeurs du libre, comme le détaillait Juergen Neumann, co-fondateur de FreiFunk :
"L'idée était de fonder une méta-communauté la plus décentralisée possible pour échanger et partager nos savoirs avec d'autres communautés en Europe et dans le monde. Nous voulions innover,

rechercher, créer, échanger, en mode DIY et open source."
Techniquement, le WiFi utilise une bande radio de faible portée surnommée "junk band" (bande poubelle), libre et gratuite. Conjuguée avec la baisse des prix de l'électronique et le talent des membres de ses communautés, ces réseaux associatifs ont permis de connecter des zones blanches dans le monde entier, du Djursland au Danemark, en passant par le Sahara et même jusque que sur le toit du monde, au Tibet. Le concept séduit aussi les collectivités locales pourvues de zones blanches. En Catalogne, Guifi.net travaille par exemple en partenariat avec des mairies.
En cohérence avec la philosophie du projet, elles développent des technologies open source et facilitent le partage de ce savoir-faire en diffusant par exemple un mode d'emploi (pdf) pour mettre en place des réseaux Freifunk en Afrique, sous licence Creative Commons ; une licence des biens communs sans fil a même été rédigée.
Dans la même état d'esprit, les FAI alternatifs "complets", proposant une connexion ADSL, se déploient aussi pour échapper aux gros telcos incontournables. Lancé au début des années 90, le French Data Network réunit ainsi aujourd'hui une vingtaine de réseaux plus ou moins avancés, pour un millier d'utilisateurs.
Rop Gonggrijp, fondateur du premier fournisseur d'accès à Internet XS4ALL, estime que ce type de structure se généralisera :
"Le FAI du futur ressemblera plus à celui des années 90. Nous nous éloignons de l'individualisme et du modèle des grandes structures et les communautés qui survivront seront celles qui auront créé leurs propres réseaux."
Il se généralisera... si le lobby des télécoms échoue à freiner le déploiement de cette fragile toile alternative. Face à une explosion du trafic mobile, qui engorge la 3G, le WiFi permet de décongestionner les tuyaux. Du coup, les gros FAI s'opposent à une ouverture gratuite des ondes, préférant mettre le grapin dessus et faire payer la facture à leurs abonnés.
Aujourd'hui, la logique propriétaire est susceptible de s'appliquer à tout, si bien que l'on oublie, pour reprendre la formule de Guy Pujolle, chercheur au CNRS, que *"les ondes radio sont un bien commun, comme l'air qu'on respire."* En face, les militants d'Open Spectrum ou de La Quadrature du Net, tentent de faire entendre leur voix libre. Malheureusement, dans ce bras de fer, les intérêts du secteur rejoignent ceux des Etats, qui peuvent vendre ces nouvelles licences, comme ils l'ont fait avec la 3G et la 4G. Et quand les caisses sont vides, que pèsent les valeurs de ces FAI associatifs ?
Les techniques se sont tellement démocratisées que des hackers envisagent très sérieusement de s'aventurer dans l'espace, une idée lancée lors du Chaos Communication Camp 2011. Déplorant que son exploration soit de plus en plus entre les mains des intérêts du privé, les hackers ont décidé de reprendre les choses en main avec le Space Program, un appel à projets. Nick Farr avait interpellé la communauté sur l'enjeu politique, par-delà le plaisir de la découverte :
"Le premier objectif est un Internet non-censurable dans l'espace. Mettons l'Internet à l'abri du contrôle des entités terrestres." L'objectif aussi est d'assurer la résilience du réseau : "La communauté hacker a besoin d'une infrastructure de repli en cas de catastrophe économique ou naturelle pour rester connectée."
En bons do-ocrates, les hackers ont mis en place le Hackerspace Global Grid (HGG) pour concrétiser leurs envies. Ils se sont joints à Constellation, une plate-forme de recherche scientifique qui met à profit les ressources d'ordinateurs en réseau. Et parce que dépasser les limites est le propre du hacker, l'objectif ultime est d'envoyer un homme dans l'espace d'ici une vingtaine d'années.

TELECOMIX, *"L'IDÉE DE LA COMMUNICATION LIBRE"*

La résilience du réseau, les hacktivistes de Telecomix connaissent sur le bout des doigts. Durant les révolutions arabes, au cours desquelles l'Internet a joué un rôle crucial dans la diffusion des informations, le collectif a enchaîné les opérations pour aider les peuples à pouvoir naviguer et

communiquer en sécurité.
Cette superbe manifestation de fraternité a marqué un premier coup d'éclat en Egypte. Le 28 janvier 2011, alors que le pays gronde, il se passe quelque chose d'inédit : Internet est coupé, à la demande du gouvernement, isolant le pays du reste de la planète. Mais le réseau n'est pas un robinet que l'on ferme d'un simple coup de poignet. Immédiatement, les hackers se mobilisent pour "rebooter" l'Internet, en mode dégradé. L'eau ne coule plus à grands flots, c'est un mince filet, mais elle coule.
Derrière l'opération, on trouve les "agents", comme ils se nomment eux-mêmes, de Telecomix. Ils forment une "désorganisation" qui agit, concrètement, en vertu de la do-ocratie, au service d'un idéal que résumait Tomate, un des agents :
"Telecomix est une idée. L'idée de la communication libre. N'importe quel type de communication."
On ne s'étonnera pas de trouver dans le lot les fils spirituels des cypherpunks de la fin des années 80...
En septembre, les Syriens bénéficient à leur tour d'une spectaculaire opération. Les internautes, qui n'ont accès qu'à un Internet censuré, sont redirigés automatiquement vers un site qui leur fournit une trousse à outil et le mode d'emploi pour contourner leur cage numérique. Ils ont récemment lancé un site rassemblant des vidéos prises sur place pour documenter les événements. Qui a dit que la jeune génération a la mémoire courte ?
Mais que les Etats occidentaux ne se drapent pas dans leurs oripeaux de pays respectueux des libertés : Telecomix aurait émergé à l'occasion du vote par le Parlement européen du Paquet Telecom, un ensemble de mesures visant à réguler les télécoms. D'abord dans une optique de lobby classique, puis dans l'entrelacs des réseaux.

WIKILEAKS, LE NAPSTER DE L'INFORMATION ? [61]

En avril 2010, le monde entier découvrait WikiLeaks avec une vidéo montrant des soldats de l'armée américaine en Irak tuant une douzaine de civils, parmi lesquels deux journalistes de Reuters, comme un joueur de jeux vidéos abattant des ennemis.
Le site, spécialisé dans la diffusion de documents confidentiels, via une plate-forme assurant l'anonymat des sources, n'en était pas à ses premières révélations. Fondé en 2006 par l'Australien Julian Assange, un ancien hacker d'obédience libertarienne, WikiLeaks avait déjà divulgué entre autres le contenu d'une boîte mail de Sarah Palin, un manuel du Pentagone sur le traitement des prisonniers de Guantanamo, les négociations en secret d'ACTA, etc. Il s'est même permis de diffuser un document de la Défense américaine où cette dernière examine les différentes tactiques possibles pour faire taire cet encombrant "whistleblower", "lanceur d'alertes".
Dans les mois qui suivent la vidéo, WikiLeaks va donner des sueurs aux grandes puissances en enchaînant trois coups d'éclats : en juillet, les War logs sur l'Afghanistan brisent la torpeur estivale avec la publication plus de 75 000 documents militaires de 2004 à 2009 ; en octobre, rebelote mais cette fois-ci avec le conflit iraquien ; enfin le petit monde feutré et discret de la diplomatie est mis à nu avec le cable gate.
Si WikiLeaks s'inscrit dans une veine déjà ancienne d'information alternative, de The Cult of the Dead Cow à Indymedia en passant par les blogs, WikiLeaks est le premier à mettre un tel bazar dans la cathédrale du journalisme d'investigation traditionnel, pour reprendre la métaphore d'Eric S. Raymond sur l'open source. De fait, les parallèles sont multiples. WikiLeaks hacke les médias, et lui-même incarne un média hacké, du moins en partie puisqu'il n'assure pas tout le travail du ressort des journalistes. Incapable de tout assumer, il s'associe avec des grands médias traditionnels et les contraint à repenser leur façon de travailler.
Face à des rédactions fermées, jalouses de leurs sources, lancées dans une course égoïste, WikiLeaks ouvre le couvercle de l'information, comme il prétend *"ouvrir les gouvernements"*. Il accompagne en cela le mouvement de l'open data, la libération des données publiques. Le temps de ces quelques grandes opérations, l'organisation force de prestigieuses rédactions à collaborer ensemble : le *New York Times*,

le *Guardian*, *Der Spiegel*, *Le Monde*, *El Pais*. Plus encore, il ouvre l'information, du moins en théorie, en proposant par exemple à n'importe qui de naviguer dans les documents, de les évaluer et de les commenter, sur le principe du crowdsourcing, comme les hackers développent et améliorent ensemble un logiciel grâce à l'accès à son code source.

The information wants to be free, WikiLeaks le rappelle brutalement, a fortiori à l'heure d'Internet : *"Il y a quelques semaines, Julian Assange, le principal porte-parole de Wikileaks, a lancé un appel aux entreprises de presse en les encourageant à mettre plus de données brutes à disposition du public"*, rappelait le journaliste Roy Greenslade, sur son blog du *Guardian*. *"Cet appel, qui a été lancé depuis la City University de Londres était entièrement orienté sur le besoin d'augmenter la transparence en matière de journalisme."*

L'autre hack spectaculaire auquel WikiLeaks se livre, c'est celui de l'attention médiatique bien sûr : à chaque nouvelle fuite, journaux, radios, télévisions et sites Internet assurent une couverture maximale. L'impact est si fort que le parallèle avec Napster est tiré : l'information ne sera plus jamais la même, WikiLeaks ouvre la porte à d'autres plates-formes du même type. Dans l'instant, la comparaison peut sembler justifiée : l'ancien porte-parole de WikiLeaks, Daniel Domscheit-Berg, part, en bisbilles, créer OpenLeaks à l'hiver 2011, avec des rédactions partenaires. La chaîne de télévision Al-Jazira lance à la même période sa Al Jazeera Transparency Unit (AJTU), le *Wall Street Journal* son Safehouse au printemps. Même les Français de *Mediapart*, peu portés sur l'innovation numérique, s'y mettent avec FrenchLeaks. On ne peut pas dire qu'ils aient particulièrement fait parler d'eux. Quant à WikiLeaks lui-même, empêtré dans ses problèmes judiciaires, d'argent et d'ego, il est loin le temps où il bouleversait l'agenda de nos gouvernants et la une de nos journaux. Ses dernières opérations, les Spyfiles, sur la surveillance du Net, et les GIFiles, des mails de la société de renseignement privé Stratfor, n'ont pas eu un écho aussi retentissant.

Du hacking, WikiLeaks a aussi emprunté certaines tares, comme le résumaient de façon cinglante Geert Lovink et Patrice Riemens.

"Thèse 7 : WikiLeaks est trop rigide. WikiLeaks est également une organisation profondément ancrée dans la culture hacker des années 80, combinée aux valeurs politiques du libertarisme technologique qui a émergé dans la décennie suivante. Le fait que WikiLeaks ait été fondé – et soit dirigé – par des geeks hardcore forme un cadre de référence essentiel pour comprendre ses valeurs et ses initiatives. Malheureusement, cet aspect va de pair avec certains aspects moins savoureux de la culture du hacking. Non pas qu'on puisse reprocher à WikiLeaks son idéalisme, son désir de faire du monde un endroit meilleur, mais plutôt le contraire. Cet idéalisme est couplé avec un appétit pour les conspirations, une attitude élitiste et un culte du secret (sans parler de mœurs condescendantes) qui sied peu à la collaboration avec des personnes possédant la même sensibilité – ainsi réduites à l'état de simples consommateurs du produit final de WikiLeaks."

Enfin, de même que le piratage des biens culturels a engendré son lot de lois répressives, WikiLeaks a produit le même effet pervers : la bataille entre l'ancien monde et le nouveau se poursuit sur le terrain de l'information.

En France, une proposition de loi a été votée début 2012 pour sanctionner la violation du "secret des affaires", avec des sanctions pénales allant jusqu'à trois ans d'emprisonnement et 375 000 euros d'amende. De quoi tarir les sources, si la loi est définivement adoptée. Aux Etats-Unis, le sénateur américain Lieberman a proposé la mise en place d'un "kill switch button", pour couper le clapet de l'Internet en cas d'urgence, ou du moins tenter de car techniquement et légalement, c'est une autre paire de manches. WikiLeaks a aussi rappelé l'importance de sécuriser ses réseaux. Aux Etats-Unis, une figure historique de la contre-culture hacker des années 80 a été embauchée pour ce job par la Darpa : Mudge, ancien adepte du culte de la vache morte, a décidé de quel côté le chapeau blanc se porte.

ANONYMOUS, SÉRIEUX COMME LE LULZ

Sur leur route, WikiLeaks et Telecomix ont croisé un collectif qui a suscité un nombre assez impressionnant de commentaires à côté du sujet. Il faut dire que les Anonymous ne facilitent pas la tâche de ceux qui aiment coller vite fait bien fait des étiquettes. Les Anons sont issus du forum d'images 4chan, foutraque pilier de la contre-culture numérique créé en 2003. Sur ce lieu fleurissent les mèmes, ces images reprises et modifiées ad libidum par les internautes, et dont le lolcat est l'exemple le plus célèbre. Les Anons ont émergé plus précisément du très trash et mythique board /b/, que l'on peut définir comme la poubelle du Net. À ce titre, le board /b/ est l'emblème d'une certaine conception du Net : un lieu où la liberté d'expression est reine et où le trolling et le lulz règnent en maître. Il n'est pas obligatoire de s'inscrire pour laisser des messages, et dans ce cas, vous êtes un "anonymous", un anonyme. Entre deux matages d'images à faire frémir Christine Boutin, les anonymous organisent des *pranks* d'un goût douteux, voire répréhensibles.

Pourtant, progressivement, une frange plus politisée se dessine à travers des actions organisées. La première, Chanology, a lieu en 2008, contre l'Eglise de scientologie, treize ans après avoir subi les foudres de CULT OF THE DEAD COW. La puissante organisation a en effet attenté à la chère liberté d'expression en tentant, en vain de faire retirer une vidéo de propagande avec Tom Cruise. Pour l'occasion, ils descendent pour la première fois dans la rue.

Depuis, les Anonymous ont multiplié les opérations en se faisant une spécialité de descendre à coups d'attaques DDoS les sites d'institutions ou d'entreprises symbolisant la répression des libertés numériques : dictatures, grosses majors du disque, lobbies ou gouvernement menant une politique anti-téléchargement. Le temps d'une opération, il lui arrive de s'associer à WikiLeaks ou Telecomix.

Anonymous impose aussi un style, entre grandiloquence théâtrale et permanente autodérision, le fameux lulz. Ironie de l'histoire, ils font les affaires du géant Time Warner : les Anons se cachent le visage derrrière un masque du révolutionnaire anglais Guy Fawkes, popularisé par le film *V comme Vendetta*, tiré de la BD de l'auteur anarchiste culte Alan Moore, dont les droits appartiennent à Time Warner. Le hacker hacké...

D'un point de vue technique, les Anonymous ne sont pas tous des hackers, seule une petite partie d'entre eux possèdent un tel bagage. Les autres apportent leur aide en fonction de leurs compétences. Pour faciliter la participation, le logiciel LOIC est mis en place en 2011, un avatar du FloodNet de l'Electronic Disturbance Theater. En cela, pour reprendre l'analyse de la socio-anthropologue Biella Coleman, les Anonymous constituent un seuil bas d'accès à la politique :

"Depuis l'hiver 2008, ce mouvement est devenu une porte d'entrée en politique pour les geeks (et consorts) qui souhaitaient passer à l'action. Entre autres opportunités, le mouvement Anonymous offre la possibilité – inédite – de mettre en place des micro–manifestations en toute discrétion, permettant à certains individus d'évoluer au sein du mouvement et de participer à des opérations d'envergure. Nul besoin de remplir le moindre formulaire, de donner son identité ou ses deniers pour avoir le sentiment de faire partie d'un vaste groupe."

Si tous les Anons ne sont pas des virtuoses de la technique, leur action collective a hacké l'attention des médias du monde entier et bien enquiquiné quelques poids lourds de ce monde. Ce qui pour une bande de geeks venus des bas-fonds de l'Internet est un exploit qui vaut bien les découvertes de failles de sécurité. Mais leurs méthodes posent de nouveau la question de ce qu'il est permis ou non de faire au nom de l'éthique hacker et quelques vieux de la vieille de l'hacktivisme, comme Oxblood Ruffin, l'ancien fondateur de Hacktivismo, leur remontent publiquement les bretelles à ce sujet : Anonymous, you've crossed the line !

Et de fait, on est en droit de leur préférer le lobbying plus propre sur lui mais sans doute plus efficace en termes de retombées concrètes de l'EFF, du CCC ou de La Quadrature du Net, qui travaillent au corps les politiques depuis 2009, année de la bataille contre la loi anti-piratage Hadopi.

HACKER LA DÉMOCRATIE

DU PIRATAGE AU PARTI PIRATE

Avec la création du Parti Pirate en 2006, un pas supplémentaire, l'ultime, est franchi : hacker la politique traditionnelle en entrant sur son terrain de jeu. En 2003, le Piratbyrån ("Bureau du piratage"), une association suédoise d'hacktivistes militant pour la légalisation du partage en ligne, lance le site de liens BitTorrent The Pirate Bay. En quelques mois, il gagne un succès considérable dans le monde entier, emmené par le trio composé de Gottfrid Svartholm Warg, Fredrik Neij et Peter Sunde, qui en devient le médiatique porte-parole.

En 2005, la Suède fait voter une loi anti-piratage, en transposition de la directive de 2001. Les lobbies, nous l'avons évoqué, s'agitent dans tous les sens et la tempête ne tarde pas à souffler sur le navire corsaire. Trop, c'est trop. Le premier eurodéputé du Parti Pirate Christian Engström se souvient :

"Le 1er janvier 2006, Rick Falkvinge, un activiste du Net, a mis en ligne une page web avec ce simple message :

« I've had enough, I'm starting the Pirate Party ».

C'était à moitié une blague, mais en 48 heures, la page a reçu trois millions de visites. Alors il s'est dit : 'bon, j'ai peut-être mis le doigt sur quelque chose...' Et il a quitté son poste de manager dans une boite d'informatique pour créer le Parti Pirate."

Dès ses premiers mois d'existence, il bénéficie d'une publicité formidable, grâce à la procédure contre The Pirate Bay. En mai 2006, les serveurs du site sont saisis, la MPAA sautille de joie mais sa joie est de courte durée puisque les serveurs sont réouverts en juin aux Pays-Bas, tandis que des centaines de personnes manifestent. Et l'on apprend au passage le lobby a fait pression sur le gouvernement suédois. Au bout de deux ans et demi d'enquête, le procès a enfin lieu en avril 2009, avec quatre administrateurs sur le banc des accusés. Les parties civiles, la MPAA et l'International Federation of the Phonographic Industry (IFPI), leur demandent environ 11 millions d'euros. De façon fort peu opportune, une nouvelle loi anti-piratage est votée pendant le procès. Le verdict est sévère, un an de prison ferme et 2,7 millions d'euros de dommages et intérêts, et un appel à la clé.

Bilan pour le Parti Pirate : dans l'immédiat, 2 000 nouveaux membres viennent renforcer ses troupes en quelques heures et le site plante, non pas victime d'une attaque DDoS mais du trop grand nombre de curieux venus se connecter ; à très court terme, aux élections européennes qui suivent en juin, ils obtiennent 7,1% des voix, ce qui leur permet d'envoyer leur premier député au Parlement.

L'ÉTHIQUE HACKER EST-ELLE SOLUBLE DANS LA DÉMOCRATIE ?

Comme le résume avec humour Rick Falkvinge dans sa présentation TEDx à Londres de mars 2012, le Parti Pirate suédois a aussi réussi un hack d'attention médiatique spectaculaire, contribuant à porter dans le débat politique leur vision du droit d'auteur, de la propriété intellectuelle et des libertés numériques bien au-delà de leurs frontières :

- *"Combien de personnes dans la salle connaissent le Parti Pirate suédois ?* (les gens lèvent la main) *Environ la moitié, les deux tiers. Et combien connaissent un parti politique suédois en dehors du Parti Pirate ?"*

Rires dans la salle, personne ne lève la main.

"Nous aimons le Net, copier, partager, et nous adorons les libertés publiques. Et pour cela, certaines personnes nous qualifient de pirates. Et plutôt que d'en avoir honte, ce qui est leur intention, nous l'avons revendiqué. Depuis, nous avons deux sièges au Parlement européen, quinze sièges au Parlement de Berlin, nous sommes présents dans 56 pays et nous avons plus de 150 élus municipaux."

Et en quelques mois, la liste des succès s'est encore allongée grâce à la montée en puissance du Parti Pirate allemand : après Berlin, il est entré dans trois autres parlements régionaux, dont celui de Rhénanie-du-Nord-Westphalie, le plus peuplé et le plus important économiquement. Il a même donné au mouvement

son premier maire, certes d'un village, mais le symbole est là.
Concrètement, comment hacke-t-on la politique ? En bon hacker -il est proche du Chaos Computer Club, l'élu berlinois Pavel Mayer envisage la politique comme un système dont il faut saisir le fonctionnement pour mieux se l'approprier : *"La machine politique du Parlement a des boutons, des leviers, que vous pouvez contrôler, vous devez comprendre ce qui se passe si vous les actionnez. On modifie la machine quand on sait exactement comment elle fonctionne."* Pavel s'est déjà attelé à cette tâche, dès la session inaugurale, fin octobre. Il a annoncé que le règlement intérieur devait évoluer afin que le parlementaire en tant qu'individu ait plus de pouvoir, car il favorise le groupe en l'état actuel : *"Cela fausse le principe de démocratie. Un élu, qui représente 20 000 citoyens, est amené à faire le choix du groupe, au lieu du sien."* Une tentative *"d' 'update', de 'patch'[62] incrémental de l'OS"* accueillie par de l'incompréhension : *"la plupart des autres élus n'ont pas compris. Ils sont là depuis 10, 20 ans, ils ne questionnent plus le système."* À la cour constitutionnelle régionale, saisie fin avril, de juger si cette update est autorisée...
Le Parti Pirate espère mettre en oeuvre le concept de "démocratie liquide", déjà à l'échelle de leur formation, qui redonne tout son sens au terme démocratie : le pouvoir du peuple. L'antenne allemande a ainsi développé le logiciel, open source bien sûr, LiquidFeedback ("retour liquide"). Grâce à cette plate-forme participative, les membres du parti peuvent faire des propositions de texte, les amender ou de faire une contre-proposition. Si l'on se sent moins compétent sur un sujet, la délégation du vote est possible. En Italie, le vote final passe aussi par cet outil.
Les hackers espagnols du collectif Hacksol ont aussi contribué activement à la réinvention des outils de la démocratie, motivés par le mouvement des Indignés en 2011 : N-1, un réseau social alternatif, pour débattre, prendre des décisions et faire circuler les contre-rendus, Take the square, une plate-forme pour relier les indignés du monde entier ou bien encore un téléphone voIP pour appeler et envoyer des sms gratuitement.
Reste à savoir qui hackera qui au final : en Espagne, la crise a eu raison des espérances d'un système alternatif et les caciques sont toujours bien en place. Nos pirates ont en mémoire le parcours des Verts, qui voulait faire de la politique autrement naguère et ont fini par faire de la politique comme tout le monde. Quant aux hackers, ils regardent pour certains avec scepticisme cette volonté de faire de la politique...

Chaos Communication Camp, août 2011. Projection de vieux épisodes de la série américaine de science-fiction, *Star Trek*, tard dans la nuit, à l'espace Baikonur. L'imagerie de la science-fiction a inspiré les décors de certains hackerspaces comme celui de C-Base à Berlin ou le Metalab de Vienne.

Sous les tentes du Chaos Communication Camp, les écrans s'activent. À deux pas de là, on danse, on joue aux jeux vidéos, on regarde des films, on partage...

La mise en scène spectaculaire au CCC, sur le site du musée de l'aviation de Finowurt au nord de Berlin, une ancienne base soviétique. Les deux grands hangars, Baikonur et Kourou accueillent les conférences.

I did it for the lulz. Je l'ai fait pour m'amuser. Dans toutes les allées du CCCamp, le même constat : on s'amuse, on expérimente, du projet le plus simple au plus élaboré comme la construction et mise en orbite de petits satellites cubes.

92.6 FM
Fri Aug 12 00:58:36 CEST 2011
-[Binary Voice - www.xenim.de
00 - 01 DJ Stitch vs DJ RevMod
01 - 02 HOAP karaoke
02 - 04 Queer Geeks
04 - 06 Political Hackers

Le Chaos Communication Camp possède sa propre station radio et plusieurs réseaux WiFi. Les ambiances sonores et visuelles changent d'une allée à l'autre, du codeur solitaire devant sa tente, à la musique électro, aux rires et conversations dans les bars, aux projections de films dans les hangars...

POSTFACE

JE SUIS UN HACKER, ET VOUS ?

Mitch Altman, que l'on a croisé plus haut, est une figure historique du hacking, co-créateur du hackerspace Noisebridge à San Francisco. Il incarne cette génération de hackers qui exerce ses talents sur les objets. Cet évangéliste inlassable parcourt le monde six mois par an pour aider au développement de la communauté, sans jamais se départir de son sourire serein. Il a accepté d'écrire la postface de cet ouvrage, où il nous livre sa vision très personnelle du hacking, intimement lié à son parcours difficile : hacker qui bat... envers et contre tout.

Mitch Altman, devant le mur de graffiti du Point FMR, lors de sa visite à Paris en février 2012.

Je suis un hacker. Et j'y prends beaucoup de plaisir. Dans le monde des hackers, j'ai trouvé une communauté, j'ai trouvé ma tribu. Vivre dans l'esprit du hacking me permet de donner un sens à ma vie. Cela marcherait peut-être avec vous aussi ? Qu'est-ce qu'un hacker ? Pour moi, c'est être capable de voir ce qui est là, d'utiliser ce qui est disponible, de l'améliorer et d'en partager les résultats. Demandez à une centaine d'autres hackers et vous aurez au moins tout autant de définitions différentes.

Nous pouvons tous en venir au monde du hacking d'une manière qui nous est propre.

J'ai grandi seul dans mon petit monde à moi. J'y ai été propulsé après avoir été brutalement persécuté parce que j'étais un geek introverti, intellectuel, louche, bizarre de bien des manières. Les professeurs de sport et d'autres figures d'autorité se tenaient debout et observaient, encourageant ainsi les injures et les sévices. Bien que ce fût douloureux, étant enfant, de voir les choses à ma façon, ça m'a aussi beaucoup servi. Ça m'a permis de trouver des solutions innovantes à des problèmes dont la plupart des personnes autour de moi n'avaient probablement pas conscience. Par nécessité, j'ai aussi appris à penser par moi-

même, à déterminer si les normes sociales signifiaient quelque chose pour moi, si les règles étaient utiles ou non. Cependant, le processus a été long et il m'a fallu beaucoup de hacking pour en arriver là.

Et pas uniquement de la technologie. Nous pouvons hacker n'importe quoi. Hacker est un mode de vie utile.

Quand j'étais petit, je ne jouais qu'avec de l'électronique, fabriquant des interphones, des bruiteurs, des jouets. J'ai construit mon propre ordinateur. J'ai créé un bang électronique. Je piratais les téléphones. Et je montrais aux autres enfants un peu geek ce que j'avais fait. Nous avons partagé nos savoirs, inspirant les uns les autres à faire plus de choses cool par le biais des super projets qu'on avait en commun. Sans le savoir à l'époque, je hackais. Nous hackions.

Avant les hackerspaces, il y eut les hackers. Et avant que les gens ne s'auto-proclament hackers, il y avait d'autres personnes qui avaient ce même état d'esprit. Socrates. Galilée. Gandhi. Ginsberg. Et des millions d'autres encore. Ces hommes très différents étaient ceux qui voyaient le monde à leur façon, et même s'ils ne s'intégraient pas dans un moule de règles et de normes, que les autres les aiment ou pas, ils montraient des choses telles qu'ils les voyaient à traves leurs lunettes. Ces personnes ont contribué de manière incroyablement positive à l'évolution de notre monde.

Avec l'essor des ordinateurs furent créés les réseaux, grâce auxquels des geeks introvertis pouvaient communiquer et explorer leurs mondes, tout en restant chez eux, à l'aide d'une ligne téléphonique. Beaucoup de ces personnes ont partagé ce qu'elles avaient appris, accroissant ainsi de manière démentielle la somme de connaissances que n'importe qui aurait pu acquérir de son côté. Certains d'entre eux se sont réunis aux premières conférences hackers. Même les geeks introvertis ont besoin de faire partie d'une communauté. Nous en avons tous besoin – c'est dans notre ADN.

Au cours des siècles, les humains ont évolué en se soutenant mutuellement, en partageant des outils efficaces qui nous ont permis de survivre et de prospérer dans des environnements parfois hostiles. Pour moi, ces premiers humains étaient eux aussi des hackers. Les hackers contemporains peuvent se servir de cette curiosité humaine innée, de notre besoin communautaire si profondément ancré, et de ce besoin tout aussi important de partager ce que nous savons, de former des communautés solidaires au sein desquelles nous pouvons tous nous développer, explorer et faire ce qui nous tient à cœur.

Nous pouvons tous en venir au monde du hacking d'une manière qui nous est propre.

J'ai grandi seul dans mon petit monde à moi. J'y ai été propulsé après avoir été brutalement persécuté parce que j'étais un geek introverti, intellectuel, louche, bizarre de bien des manières. Les professeurs de sport et d'autres figures d'autorité se tenaient debout et observaient, encourageant ainsi les injures et les sévices. Bien que ce fût douloureux, étant enfant, de voir les choses à ma façon, ça m'a aussi beaucoup servi. Ça m'a permis de trouver des solutions innovantes à des problèmes dont la plupart des personnes autour de moi n'avaient probablement pas conscience. Par nécessité, j'ai aussi appris à penser par moi-même, à déterminer si les normes sociales signifiaient quelque chose pour moi, si les règles étaient utiles ou non. Cependant, le processus a été long et il m'a fallu beaucoup de hacking pour en arriver là.

Et pas uniquement de la technologie. Nous pouvons hacker n'importe quoi. Hacker est un mode de vie utile.

Quand j'étais petit, je ne jouais qu'avec de l'électronique, fabriquant des interphones, des bruiteurs, des jouets. J'ai construit mon propre ordinateur. J'ai créé un bang électronique. Je piratais les téléphones. Et je montrais aux autres enfants un peu geek ce que j'avais fait. Nous avons partagé nos savoirs, inspirant les uns les autres à faire plus de choses cool par le biais des super projets qu'on avait en commun. Sans le savoir à l'époque, je hackais. Nous hackions.

Avant les hackerspaces, il y eut les hackers. Et avant que les gens ne s'auto-proclament hackers, il y avait d'autres personnes qui avaient ce même état d'esprit. Socrates. Galilée. Gandhi. Ginsberg. Et des millions d'autres encore.

Ces hommes très différents étaient ceux qui voyaient le monde à leur façon, et même s'ils ne s'intégraient

pas dans un moule de règles et de normes, que les autres les aiment ou pas, ils montraient des choses telles qu'ils les voyaient à traves leurs lunettes. Ces personnes ont contribué de manière incroyablement positive à l'évolution de notre monde.

Le hack le plus important de ma vie a été de me hacker moi-même. Bien sûr, je me suis planté - lamentablement au début. Qu'est-ce que je savais ? Tout ce que je savais c'était que la vie n'était rien d'autre que dépression, me blâmant moi-même pour tout ce gâchis, et je voulais que la douleur cesse. C'était une force plutôt motivante ! J'ai appris de mes erreurs. Faire des choix en pensant qu'ils arrangeraient les choses. Me planter encore un peu plus. Faire de nouveaux choix. Souffrir des conséquences de ces mauvais choix. Apprendre. Faire de nouveaux choix. Finir par apprendre à faire de meilleurs choix pour moi et pour ceux qui m'entourent. Plus de choix. Apprendre. Finir par apprendre à être heureux, et vivre une vie que j'aime. Nous pouvons hacker nos vies !

Nous pouvons hacker la société. Le règlement de votre lycée vous empêche de faire quelque chose de super cool ? Peut-être qu'un professeur sympa serait prêt à remplir quelques formulaires que vous pourrez arranger à votre sauce pour créer un événement – c'est comme ça que mes amis et moi avons créé l'"embouteillage du déjeuner", on mettait un peu d'équipement son dans le hall, et plusieurs groupes jouaient du rock, ce qui pouvait durer jusque dans l'après-midi. Le sport ça craint ? Peut-être que votre professeur d'arts plastiques peut signer quelques formulaires supplémentaires que vous pouvez contourner un peu pour tourner un film durant cette période d'enfer. Ensuite vous pouvez projeter le film de votre propre vision de l'école à la fête de fin d'année. Vous n'appartenez à aucune communauté dans votre ville ?

Imaginez la culture dans laquelle vous aimeriez baigner, faites passer le message. Ca va attirer les personnes qui s'y intéressent, ce qui va permettre d'améliorer cette culture, d'attirer plus de personnes, ne reste plus qu'à louer un endroit pour vous retrouver. Voilà ! Vous venez de créer une communauté à partir de rien ! Vous avez créé un hackerspace – où les gens peuvent explorer, faire ce qu'ils aiment, enseigner, apprendre, partager, évoluer.

Nous pouvons hacker n'importe quoi ! En agissant de la sorte, nous contribuons peut-être à faire de notre monde un monde meilleur. Ça vaut le coup d'essayer non ? Ça ne dépend plus que de vous.

Les robots ferrailleurs du Tetalab, le hackerspace de Toulouse, dans ses locaux partagés avec le collectif d'artistes Mix'art Myris.

QUELQUES RÉFÉRENCES

Loyd Blankeship, *La conscience d'un hacker*
Chaos Computer Club, *The hacker bible*
Cory Doctorow, *Makers*, disponible en téléchargement libre ou édition papier Tor Books (Etats-Unis) et HarperVoyager (Royaume-Uni), 2009.
Pekka Himanen, Linus Torvalds, Manuel Castells, *The hacker ethic*, Random house, 2001.
Timothy Leary, *Chaos et cyberculture*, 1994, 1996 pour la version française aux Editions du Lézard (épuisée).
Steve Levy, *Hackers, heroes of the computer revolution*, Doubleday, 1984, édition anniversaire augmentée pour les vingt-cinq ans, O'Reilly, 2010.
Eric S. Raymond, *The jargon files*
Eric S. Raymond, *Comment devenir un hacker* (version originale)
Eric S. Raymond, *La cathédrale et le bazar* (version originale)
Etienne Rouillon et Sylvain Bergère, *Pir@tage*, documentaire diffusé sur France 4 en 2011.
Richard Matthew Stallman, Sam Williams et Christophe Masutti, *Richard Stallman et la révolution du logiciel libre*
Bruce Sterling, *The Hacker crackdown, Law and disorder on the electronic frontier*, disponible en téléchargement gratuit, Bantam Books, 1992.
Fred Turner, *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*, University of Chicago Press, 2006.
Philip Zimmermann, *Pourquoi j'ai créé PGP*

REMERCIEMENTS

Les Owniens, en particulier Guillaume Ledit, éthique media hacker, Jean-Marc Manach, “petit pied” des Internets français, qui nous a ouvert au monde merveilleux des hackers, Pierre “icono” Alonso, Marie Coussin pour sa relecture et Anaïs Richardin pour son support traduction. Mitch Altman, prodigue roi du fer à souder ; Christophe Masutti, fin libriste ; C-ven de C-Base à Berlin, C3o du Metalab de Vienne, Stefan du HSBP de Budapest, Nusepas et l’équipe de Guifinet en Catalogne pour leur accueil. Julien “Archiloque” Kirch ; papa-maman, en espérant que vous compreniez mieux pourquoi on vous casse les oreilles avec nos hackers #oupas.
Ce livre n’est pas dédié à Thierry Lhermitte et Marie-Françoise Marais.

NOTES

[1] Voir le chapitre 3 Internet, terrain de bataille grand public, Et l'argent coule de source.
[2] La citation exacte, attribué à Stewart Brand, que l'on croisera un peu plus loin, est : *"Information wants to be free. Information also wants to be expensive. ...That tension will not go away."* Les hackers penchent définitivement du premier côté.
[3] Sur l'éthique hacker, lire Steven Levy, *Hackers, Heroes of the computer revolution*, chapitre 2. Publié en 1984, cet ouvrage est le premier qui rend hommage au rôle des hackers dans l'histoire de l'informatique, et constitue une référence incontournable sur le sujet ; et Pekka Himanen, Linus Torvalds, Manuel Castells, *The hacker ethic*.
[4] Pir@tages, Etienne Rouillon et Sylvain Bergère, documentaire diffusé sur France 4 en 2011.
[5] Source : Framablog, *"Socrate et les hackers - Une conférence de Bernard Stiegler"* ; la conférence en question est lumineuse.
[6] Eric S. Raymond, *Comment devenir un hacker* ; version originale).
[7] Les citations de cette sous-partie sont extraites de l'ouvrage de Steven Levy. Voir note supra.
[8] La sérendipité désigne les découvertes que l'on fait en se laissant guider par sa curiosité. Ce phénomène est particulièrement propre à Internet, quand nous sautons de lien en lien en déviant de notre recherche initiale. Lire à ce sujet cet article d'InternetActu.
[9] Voir le chapitre 2 En résistance, et les sous-chapitres Le Chaos Computer Club et En défense du Far West
[10] Dans *"The origin of Spacewar"*, publié en 1981 dans le magazine Creative Computing, Martin Graetz revient en détail sur l'histoire de *Spacewar!* Vous pouvez revivre les sensations de jeu de l'époque avec ce simulateur.
[11] Voir les sous-chapitres Le phreak, c'est chic et Des jeunes gens dans un garage.
[12] Source Steven Levy, *Heroes of the computer revolution*
[13] Source *ibidum*
[14] Voir le chapitre 4 Hackers on planet earth et le sous-chapitre L'hacktivisme en ouverture des JT
[15] Lire *"Aux origines de la cyberculture : LSD et HTML"* ; Timothy Leary, *Chaos et cyberculture* ; Fred Turner, *From counterculture to cyberculture*.
[16] Voir note précédente.
[17] Internet, terrain de bataille grand public.
[18] *Ibidum*.
[19] Source Steven Levy.
[20] *"An open letter to hobbyists"*. Les discussions sur la légitimité de sa position sont particulièrement intéressantes.
[21] Voir le chapitre 2 En résistance, et le sous-chapitre Libre !
[22] Interview de 1995 par Tom Barbalet.
[23] *Tap* et *2600* sont deux fanzines fameux consacrés au hacking et en particulier le phreaking.
[24] Chronologie complète sur le site d'UNIX.
[25] Source
[26] *The Arpanet Completion report*, Bolt, Beranek et Newman, 1978, cité dans *Behind the Net - The untold history of the ARPANET Or - The "Open" History of the ARPANET/Internet*, Michael Hauben
[27] Source *Ibidum*
[28] Source : *The Art of UNIX Programming*, Chapitre 2, Histoire.
[29] *Confessions d'un voleur Internet, la liberté confisquée*.

[30] Echange par mail avec l'auteur.
[31] Voir le chapitre 4 Hackers on planet earth, et les sous-chapitres Anonymous, et, Sérieux comme le lulz
[32] Bruce Sterling, *The Hacker crackdown, Law and disorder on the electronic frontier*.
[33] Nous n'avons pas traduit le terme "privacy", car son sens est plus complexe que "vie privée", il comprend aussi la notion d'intimité.
[34] Source : *Le manifeste crypto-anarchiste*.
[35] Source : *A Cypherpunk's manifesto*.
[36] Source : *Le manifeste crypto-anarchiste*.
[37] Voir le chaptire 3 Internet, terrain de bataille grand public, et le sous-chapitre L'essor de l'hacktivisme.
[38] Source *Pir@tage*, Etienne Rouillon et Sylvain Bergère, documentaire diffusé sur France 4 en 2011.
[39] Voir par exemple l'histoire de Karl Koch, retrouvé "suicidé" dans une forêt, brûlé à l'essence, après avoir collaboré avec le KGB.
[40] Source.
[41] Source *Richard Matthew Stallman, Sam Williams et Christophe Masutti, Richard Stallman et la révolution du logiciel libre*, chapitre 7, Une morale à l'épreuve.
[42] *Ibidum.*
[43] Certains rangent Tim Berners-Lee dans la catégorie des hackers, ce qui se défend. Pour notre part, nous considérons qu'il est dans une démarche classique de chercheur dans le rang, certes génial et ardent défenseur des libertés numériques, mais pas assez "de côté" pour être un hacker.
[44] Andrew S. Tanenbaum justifiera son choix dans un long échange avec son élève dissident : *"Les limites de MINIX sont en partie imputables à mon coté professeur : le but explicite de sa conception était de le faire fonctionner sur du matériel bon marché pour que les étudiants puissent se le payer. [...] Faire des logiciels gratuits mais seulement pour des types qui ont assez d'argent pour se payer du matériel hors de prix est un concept intéressant."*
[45] Source *Richard Matthew Stallman, Sam Williams et Christophe Masutti, Richard Stallman et la révolution du logiciel libre*, chapitre 10, Gnu/Linux.
[46] Une distribution est un noyau Linux complété par un ensemble de logiciels.
[47] Source *"Le pragmatiste du logiciel libre : entretien avec Linus Torvalds"*.
[48] En droit américain, le *fair use*, littéralement "usage équitable, raisonnable", désigne les exceptions au droit d'auteur, visant à assurer un équilibre entre ce dernier et le public.
[49] Source *"Comment la crainte de sous-protection engendrera la catastrophe de la surprotection : examen constitutionnel du Digital Millenium Copyright Act"* Remy Khouzam, 2004.
[50] Sources : *"'Mom, I blew up the music industry'" ; "With a little help from his friends" ; "The day the Napster died"*.
[51] L'interface de programmation de Windows.
[52] Voir le chapitre 4 Hackers on planet Earth, et le sous-chapitre Anonymous, sérieux comme le lulz.
[53] Nous empruntons ce titre à la conférence du même nom, HOPE en abrégé.
[54] Nous empruntons ce titre à l'article de Jean-Marc Manach paru sur *InternetActu*.
[55] Lire Makers (1/2) : *Faire société* et Makers (2/2) : *Refabriquer la société*.
[56] Source : Entretien avec Hackable Devices, site de diffusion massive de matériel libre et présentation sur Bearstech, structure coopérative qui porte l'entreprise.
[57] Une revue plus détaillée dans cet article de *Make magazine* "*Open source hardware what is it? Here's a start."*
[58] *Makers*, du journaliste et romancier Cory Doctorow, est une fiction décrivant l'émergence d'une économie du hardware hacking.

[59] La conférence a été présentée de nouveau lors du Chaos Communication Congress l'hiver suivant.
[60] La sécurité de Tor est un débat récurrent dans le milieu.
[61] Outre de nombreux articles et applications sur ce sujet, Owni a publié *La véritable histoire de WikiLeaks*, d'Olivier Tesquet.
[62] En informatique, un patch est une correction apportée à un bug sur un programme.

SABINE BLANC - OPHELIA NOOR

HACKERS: BÂTISSEURS DEPUIS 1959

"Le contournement intelligent des limites imposées,
qu'elles le soient par votre gouvernement, vos propres capacités ou les lois de la physique."

Jude Milhon, "St. Jude", patronne des hackers, 1939-2003

RETROUVEZ
TOUTES NOS ÉDITIONS
SUR OWNI-EDITIONS.COM

SOCIÉTÉ POUVOIRS
ET CULTURES NUMÉRIQUES
SUR OWNI.FR

© OWNI - ÉDITIONS
Photographies : Ophelia Noor
Texte : Sabine Blanc

ISBN 979-10-90473-25-6

OWNI
ÉDITIONS

Réalisation au format ePub

www.igs-cp.fr

Fichier testé et optimisé pour les applications iBooks v.2.2 et Adobe Digital Edition v.1.7.2